PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-244926

(43)Date of publication of application : 30.08.2002

(51)Int.Cl. G06F 12/14
G06F 17/60
H04L 9/08
H04N 5/765
H04N 5/781
H04N 5/85
H04N 5/91

(21)Application number : 2001-039140

(22)Date of filing : 15.02.2001

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

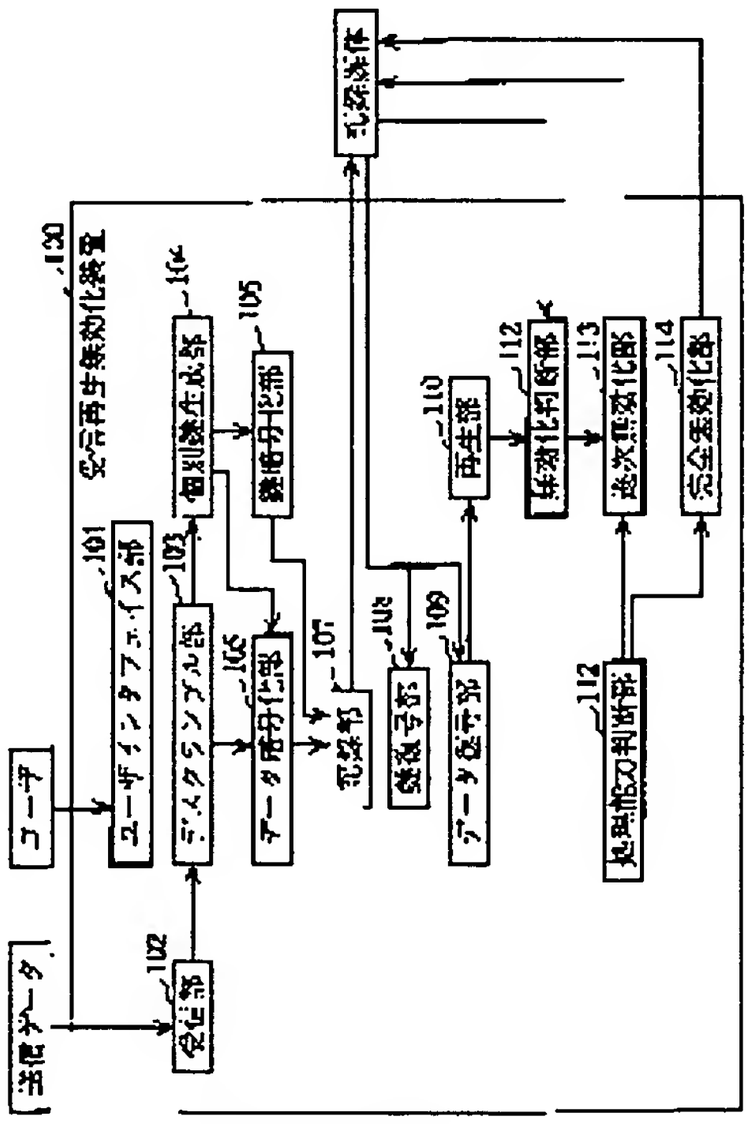
(72)Inventor : MURASE KAORU
MOTOHASHI YOSHIHIKO
MIYAZAKI MASAYA

(54) DATA INVALIDATING DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a data invalidating device capable of improving user's convenience without deviating from the purpose allowing no duplicate of data.

SOLUTION: This data invalidating device is provided with a receiving part 102 for receiving the data indicating that copying is not permitted, a recording part 107 dividing the received data into partial data and recording it, a reproducing part 110 for reproducing the recorded partial data sequentially, an invalidation judging part 111 judging that the partial data must be invalidated due to the expiration of recording term and the reproduction of the partial data, and a one after another invalidating part 113 for destroying at least the data required previously to utilize other data among the partial data to be invalidated one after another by substituting new data and arbitrary data.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2002－244926
（P2002－244926A）
(43)公開日　平成14年８月30日(2002.8.30)

(51)Int.Cl.⁷		識別記号	FI		テーマコード(参考)	
Ｇ０６Ｆ	12/14	３２０	Ｇ０６Ｆ	12/14	３２０Ｄ	５Ｂ０１７
					３２０Ｅ	５Ｃ０５２
	17/60	１４２		17/60	１４２	５Ｃ０５３
Ｈ０４Ｌ	9/08		Ｈ０４Ｎ	5/85	Ｚ	５Ｊ１０４
Ｈ０４Ｎ	5/765		Ｈ０４Ｌ	9/00	６０１Ｃ	

審査請求　未請求　請求項の数39　ＯＬ　（全 24 頁）　最終頁に続く

(21)出願番号　特願2001－39140(P2001－39140)

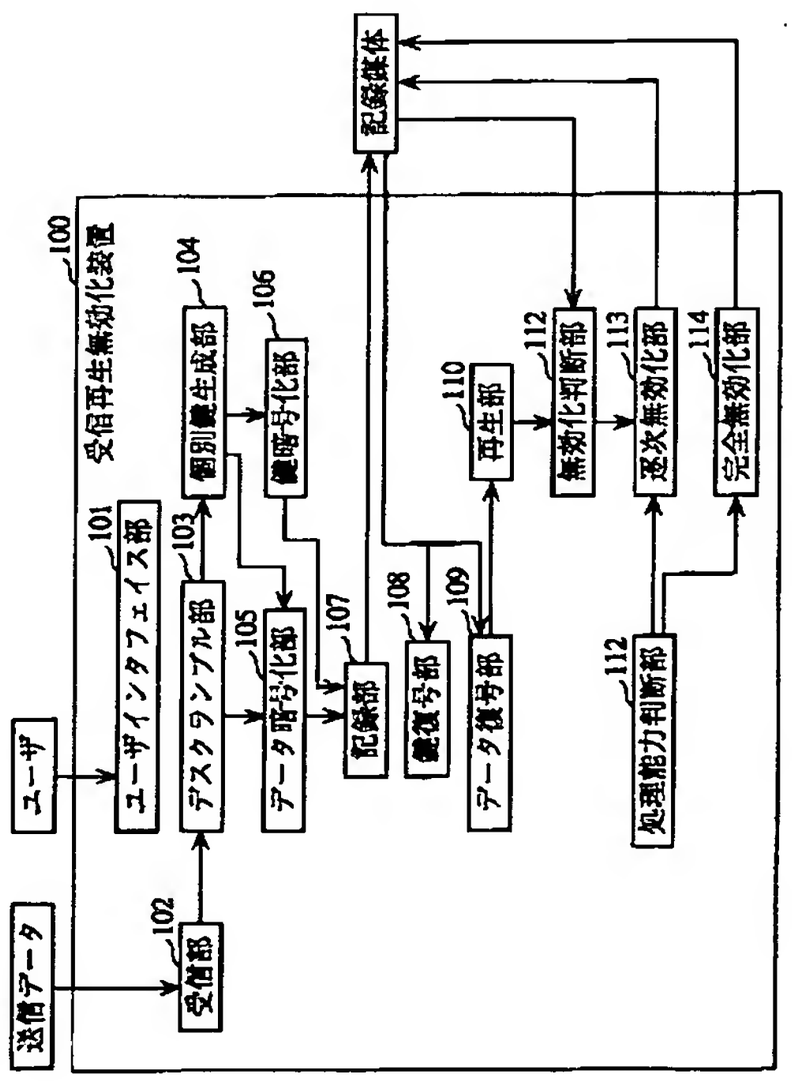
(22)出願日　平成13年２月15日(2001.2.15)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　村瀬　薫
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　本橋　良彦
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100090446
弁理士　中島　司朗

最終頁に続く

(54)【発明の名称】　データ無効化装置

(57)【要約】
【課題】データの複製品を許さないという趣旨を逸脱せずにユーザの利便性を向上させることができるデータ無効化装置を提供する。
【解決手段】コピー不可を示すデータを受信する受信部１０２と、受信されたデータを部分データに分けて記録する記録部１０７と、記録された部分データを順次再生する再生部１１０と、記録期限が切れた事や再生された事等をもって部分データを無効化すべきと判断する無効化判断部１１１と、無効化すべき部分データのうち少なくとも他のデータを利用するために先に必要となるデータを、新しいデータや任意のデータを上書きする等して逐次破壊する逐次無効化部１１３とを備える。



1

【特許請求の範囲】

【請求項１】　一の記録媒体に記録された対象データを無効化するデータ無効化装置であって、
前記対象データは、複数の部分データから構成され、
前記部分データ単位で前記一の記録媒体に記録された対象データを、無効化すべきか否か判断する判断手段と、
前記判断手段により所定数又は所定量の部分データに対して無効化すべきと判断される度に、前記一の記録媒体に記録された対象データのうちの、当該無効化すべきと判断された部分データを逐次無効化する逐次無効化手段とを備えることを特徴とするデータ無効化装置。

【請求項２】　前記一の記録媒体は、記録された各部分データの記録順序を示す順序情報を記録しており、
前記判断手段は、前記順序情報により示される記録順序に基づいて、先に記録された部分データから順番に無効化すべきと判断することを特徴とする請求項１に記載のデータ無効化装置。

【請求項３】　前記一の記録媒体に記録されている対象データは、他の装置から連続的に送信される送信データが、現在の分まで継続的に記録されているものであり、
前記データ無効化装置は、さらに、
前記送信データを受信する受信手段を備え、
前記逐次無効化手段は、
受信手段により受信された送信データを新たな部分データとし、前記一の記録媒体内の前記判断手段により無効化すべきと判断された部分データが記録されている記録領域に、前記新たな部分データを上書きすることにより、当該新しい部分データを記録しつつ当該無効化すべきと判断された部分データを無効化することを特徴とする請求項２に記載のデータ無効化装置。

【請求項４】　前記部分データはそれぞれ、前記送信データの一定の送信時間分のデータであり、
前記一の記録媒体には、前記一定の送信時間分のデータを記録するための記録領域が規定数だけ確保されることを特徴とする請求項３に記載のデータ無効化装置。

【請求項５】　前記一定の送信時間分のデータが、常に一定のデータ量でない場合において、
前記逐次無効化手段は、前記無効化すべきと判断された部分データのうち、前記新たな部分データを上書きするだけでは全て上書きできない部分に、さらに、任意のデータを上書きすることを特徴とする請求項４に記載のデータ無効化装置。

【請求項６】　前記逐次無効化手段は、前記新たな部分データの上書きを止めた後も、先に記録されている部分データを全て無効化するまでは、任意のデータを継続的に上書きすることを特徴とする請求項４及び５の何れか１項に記載のデータ無効化装置。

【請求項７】　前記一の記録媒体には、記録された各部分データの記録期限を管理するための期限管理情報が記録されており、

2

前記判断手段は、前記期限管理情報に基づいて、記録期限が切れた部分データを無効化すべきと判断することを特徴とする請求項１に記載のデータ無効化装置。

【請求項８】　前記データ無効化装置は、さらに、
前記一の記録媒体に記録された対象データを、前記部分データ単位で利用する利用手段を備え、
前記判断手段は、さらに、前記利用手段により利用された部分データを無効化すべきと判断することを特徴とする請求項２及び７の何れか１項に記載のデータ無効化装置。

【請求項９】　前記データ無効化装置は、さらに、
前記一の記録媒体に記録された対象データを、前記部分データ単位で利用する利用手段を備え、
前記判断手段は、前記利用手段により利用された部分データを無効化すべきと判断することを特徴とする請求項１に記載のデータ無効化装置。

【請求項１０】　前記一の記録媒体に記録されている対象データは、他の装置から送信されたコンテンツデータが記録されているものであり、
前記送信されたコンテンツデータには、前記対象データのコピーの可否を示すコピー制御情報が添付されており、
前記利用手段は、前記一の記録媒体に記録されたコンテンツデータを、前記部分データ単位で再生するものであり、
前記判断手段は、前記送信されたコンテンツデータに添付されていたコピー制御情報がコピー不可を示していた場合に限り、前記利用手段により再生された部分データに対応する、前記一の記録媒体に記録された部分データを無効化すべきと判断をすることを特徴とする請求項８及び９の何れか１項に記載のデータ無効化装置。

【請求項１１】　前記一の記録媒体に記録されている対象データには、前記対象データのコピーの可否を示すコピー制御情報が添付されており、
前記利用手段は、前記一の記録媒体に記録された対象データを、前記部分データ単位で、二の記録媒体に記録するものであり、
前記判断手段は、前記コピー制御情報がコピー不可を示している場合に限り、前記利用手段により前記二の記録媒体に記録された部分データに対応する、前記一の記録媒体に記録された部分データを無効化すべきと判断をすることを特徴とする請求項９に記載のデータ無効化装置。

【請求項１２】　前記逐次無効化手段は、
前記一の記録媒体上の、前記判断手段により無効化すべきと判断された部分データを全て逐次破壊することを特徴とする請求項１～１１の何れか１項に記載のデータ無効化装置。

【請求項１３】　前記逐次無効化手段は、
前記一の記録媒体上の、前記判断手段により無効化すべ

きと判断された部分データのうちの、部分データを利用する際に、他のデータを利用するために先に必要となるデータを、少なくとも逐次破壊することを特徴とする請求項１、２及び７～１１の何れか１項に記載のデータ無効化装置。

【請求項１４】　前記一の記録媒体に記録されている対象データは、Ｉピクチャーを含むＭＰＥＧデータであり、

前記先に必要となるデータは、Ｉピクチャーであることを特徴とする請求項１３に記載のデータ無効化装置。

【請求項１５】　前記一の記録媒体に記録されている対象データは、Ｉピクチャーを含むＭＰＥＧデータであり、

前記先に必要となるデータは、Ｉピクチャーの先頭のセクタであることを特徴とする請求項１３に記載のデータ無効化装置。

【請求項１６】　前記逐次無効化手段は、

自身の処理能力に余裕が無い場合には、前記少なくとも逐次破壊するとした部分のデータのみを逐次破壊することを特徴とする請求項１３～１５の何れか１項に記載のデータ無効化装置。

【請求項１７】　前記逐次無効化手段は、

自身の処理能力の余裕の範囲で、前記少なくとも破壊するとした部分以外のデータを破壊することを特徴とする請求項１６に記載のデータ無効化装置。

【請求項１８】　前記データ無効化装置は、さらに、

前記無効化すべきと判断された部分データのうち、前記逐次無効化手段により逐次破壊されなかった部分のデータを、前記処理能力に余裕がある時に全て破壊する完全無効化手段を備えることを特徴とする請求項１６及び１７の何れか１項に記載のデータ無効化装置。

【請求項１９】　前記一の記録媒体に記録されている対象データは、前記部分データ毎に個別の部分データ暗号鍵を用いて暗号化されており、

前記一の記録媒体には、暗号化され記録された各部分データを復号するための各部分データ復号鍵が記録されており、

前記逐次無効化手段は、

前記一の記録媒体上の、前記判断手段により無効化すべきと判断された部分データに対応する部分データ復号鍵を、少なくとも逐次破壊することを特徴とする請求項１、２及び７～１１の何れか１項に記載のデータ無効化装置。

【請求項２０】　前記データ無効化装置は、さらに、

暗号化された前記対象データを入手する入手手段と、

入手手段により入手された暗号化された対象データを、正当な使用者に予め配布された使用者鍵を用いて復号し、対象データを生成する復号手段と、

前記部分データ毎に、任意の部分データ暗号鍵と、対応する部分データ復号鍵とを生成する鍵生成手段と、

復号手段により復号された対象データを、前記部分データ毎に、鍵生成手段により生成された部分データ暗号鍵を用いて、対応する部分データ復号鍵によって復号可能に暗号化するデータ暗号化手段と、

鍵生成手段により生成された部分データ復号鍵を、当該データ無効化装置に固有の識別子を用いて暗号化する鍵暗号化手段と、

データ暗号化手段により暗号化された部分データと、対応する鍵暗号化手段により暗号化された部分データ復号鍵とを、前記一の記録媒体に記録する記録手段とを備えることを特徴とする請求項１９に記載のデータ無効化装置。

【請求項２１】　前記データ無効化装置は、

少なくとも、前記復号手段、前記鍵生成手段、前記データ暗号化手段、及び、鍵暗号化手段を、同一の半導体チップ内に収めることを特徴とする請求項２０に記載のデータ無効化装置。

【請求項２２】　一の記録媒体に記録された対象データを無効化するデータ無効化プログラムであって、

前記対象データは、複数の部分データから構成され、

コンピュータに、

前記部分データ単位で前記一の記録媒体に記録された対象データを、無効化すべきか否か判断する判断ステップと、

前記判断ステップにより所定数又は所定量の部分データに対して無効化すべきと判断される度に、前記一の記録媒体に記録された対象データのうちの、当該無効化すべきと判断された部分データを逐次無効化する逐次無効化ステップとを実行させることを特徴とするデータ無効化プログラム。

【請求項２３】　前記一の記録媒体は、記録された各部分データの記録順序を示す順序情報を記録しており、

前記判断ステップは、前記順序情報により示される記録順序に基づいて、先に記録された部分データから順番に無効化すべきと判断することを特徴とする請求項２２に記載のデータ無効化プログラム。

【請求項２４】　前記一の記録媒体に記録されている対象データは、他の装置から連続的に送信される送信データが、現在の分まで継続的に記録されているものであり、

前記データ無効化プログラムは、さらに、

コンピュータに、

前記送信データを受信する受信ステップを実行させ、

前記逐次無効化ステップは、

受信ステップにより受信された送信データを新たな部分データとし、前記一の記録媒体内の前記判断ステップにより無効化すべきと判断された部分データが記録されている記録領域に、前記新たな部分データを上書きすることにより、当該新しい部分データを記録しつつ当該無効化すべきと判断された部分データを無効化することを特

徴とする請求項２３に記載のデータ無効化プログラム。

【請求項２５】　前記一の記録媒体には、記録された各部分データの記録期限を管理するための期限管理情報が記録されており、

前記判断ステップは、前記期限管理情報に基づいて、記録期限が切れた部分データを無効化すべきと判断することを特徴とする請求項２２に記載のデータ無効化プログラム。

【請求項２６】　前記データ無効化プログラムは、さらに、

コンピュータに、

前記一の記録媒体に記録された対象データを、前記部分データ単位で利用する利用ステップを実行させ、

前記判断ステップは、さらに、前記利用ステップにより利用された部分データを無効化すべきと判断することを特徴とする請求項２３及び２５の何れか１項に記載のデータ無効化プログラム。

【請求項２７】　前記データ無効化プログラムは、さらに、

コンピュータに、

前記一の記録媒体に記録された対象データを、前記部分データ単位で利用する利用ステップを実行させ、

前記判断ステップは、前記利用ステップにより利用された部分データを無効化すべきと判断することを特徴とする請求項２２に記載のデータ無効化プログラム。

【請求項２８】　前記逐次無効化ステップは、

前記一の記録媒体上の、前記判断ステップにより無効化すべきと判断された部分データを全て逐次破壊することを特徴とする請求項２２～２７の何れか１項に記載のデータ無効化プログラム。

【請求項２９】　前記逐次無効化ステップは、

前記一の記録媒体上の、前記判断手段により無効化すべきと判断された部分データのうちの、部分データを利用する際に、他のデータを利用するために先に必要となるデータを、少なくとも逐次破壊することを特徴とする請求項２２、２３及び２５～２７の何れか１項に記載のデータ無効化プログラム。

【請求項３０】　前記一の記録媒体に記録されている対象データは、前記部分データ毎に個別の部分データ暗号鍵を用いて暗号化されており、

前記一の記録媒体には、暗号化され記録された各部分データを復号するための各部分データ復号鍵が記録されており、

前記逐次無効化ステップは、

前記一の記録媒体上の、前記判断手段により無効化すべきと判断された部分データに対応する部分データ復号鍵を、少なくとも逐次破壊することを特徴とする請求項２２、２３及び２５～２７の何れか１項に記載のデータ無効化プログラム。

【請求項３１】　一の記録媒体に記録された対象データを無効化するデータ無効化方法であって、

前記対象データは、複数の部分データから構成され、

前記部分データ単位で前記一の記録媒体に記録された対象データを、無効化すべきか否か判断する判断ステップと、

前記判断ステップにより所定数又は所定量の部分データに対して無効化すべきと判断される度に、前記一の記録媒体に記録された対象データのうちの、当該無効化すべきと判断された部分データを逐次無効化する逐次無効化ステップとを備えることを特徴とするデータ無効化方法。

【請求項３２】　前記一の記録媒体は、記録された各部分データの記録順序を示す順序情報を記録しており、

前記判断ステップは、前記順序情報により示される記録順序に基づいて、先に記録された部分データから順番に無効化すべきと判断することを特徴とする請求項３１に記載のデータ無効化方法。

【請求項３３】　前記一の記録媒体に記録されている対象データは、他の装置から連続的に送信される送信データが、現在の分まで継続的に記録されているものであり、

前記データ無効化方法は、さらに、

前記送信データを受信する受信ステップを備え、

前記逐次無効化ステップは、

受信ステップにより受信された送信データを新たな部分データとし、前記一の記録媒体内の前記判断ステップにより無効化すべきと判断された部分データが記録されている記録領域に、前記新たな部分データを上書きすることにより、当該新しい部分データを記録しつつ当該無効化すべきと判断された部分データを無効化することを特徴とする請求項３２に記載のデータ無効化方法。

【請求項３４】　前記一の記録媒体には、記録された各部分データの記録期限を管理するための期限管理情報が記録されており、

前記判断ステップは、前記期限管理情報に基づいて、記録期限が切れた部分データを無効化すべきと判断することを特徴とする請求項３１に記載のデータ無効化方法。

【請求項３５】　前記データ無効化方法は、さらに、

前記一の記録媒体に記録された対象データを、前記部分データ単位で利用する利用ステップを備え、

前記判断ステップは、さらに、前記利用ステップにより利用された部分データを無効化すべきと判断することを特徴とする請求項３２及び３４の何れか１項に記載のデータ無効化方法。

【請求項３６】　前記データ無効化方法は、さらに、

前記一の記録媒体に記録された対象データを、前記部分データ単位で利用する利用ステップを備え、

前記判断ステップは、前記利用ステップにより利用された部分データを無効化すべきと判断することを特徴とする請求項３１に記載のデータ無効化方法。

【請求項３７】　前記逐次無効化ステップは、
前記一の記録媒体上の、前記判断ステップにより無効化すべきと判断された部分データを全て逐次破壊することを特徴とする請求項３１～３６の何れか１項に記載のデータ無効化方法。
【請求項３８】　前記逐次無効化ステップは、
前記一の記録媒体上の、前記判断手段により無効化すべきと判断された部分データのうちの、部分データを利用する際に、他のデータを利用するために先に必要となるデータを、少なくとも逐次破壊することを特徴とする請求項３１、３２及び３４～３６の何れか１項に記載のデータ無効化方法。
【請求項３９】　前記一の記録媒体に記録されている対象データは、前記部分データ毎に個別の部分データ暗号鍵を用いて暗号化されており、
前記一の記録媒体には、暗号化され記録された各部分データを復号するための各部分データ復号鍵が記録されており、
前記逐次無効化ステップは、
前記一の記録媒体上の、前記判断手段により無効化すべきと判断された部分データに対応する部分データ復号鍵を、少なくとも逐次破壊することを特徴とする請求項３１、３２及び３４～３６の何れか１項に記載のデータ無効化方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、データの著作権を保護する為にデータを無効化する装置に関し、特に、著作権を保護しつつ、ユーザの利便性を高める技術に関する。
【０００２】
【従来の技術】近年、情報のデジタル化が進んでいる。デジタル化された情報（以下「デジタルコンテンツ」と言う）は時間とともに劣化することがなく、また比較的取り扱い易いので、特に音声情報や画像情報のデジタル化が著しく進んでいる。しかしデジタルコンテンツはコピーしてもオリジナルと全く同じものができるので、著作権のある情報が無断で複製されたり、改ざんされたりといった不正行為が簡易に行なわれてしまうという欠点を持っている。
【０００３】このような不正行為を防ぐために、デジタルコンテンツを暗号化して供給し、著作権料を支払う契約をしているような正当なユーザの装置のみに復号の為の復号鍵を付与する方法が考えられる（以下、暗号化されたデジタルコンテンツを「暗号化コンテンツ」と言う）。このようにすると、正当なユーザの装置以外の他の装置では暗号化コンテンツを復号できないのでデジタルコンテンツの不正な使用を防ぐことができる。
【０００４】また、著作権保護の要否を示すために、デジタルコンテンツにはコピーの可否等を示すコピー制御

情報（ＣＣＩ：Ｃｏｐｙ　Ｃｏｎｔｒｏｌ　Ｉｎｆｏｒｍａｔｉｏｎ）を添付することがある。コピー制御情報は、「Ｃｏｐｙ　Ｎｅｖｅｒ」、「Ｃｏｐｙ　ｏｎｅ　Ｇｅｎｅｒａｔｉｏｎ」、「Ｃｏｐｙ　Ｎｏ　ｍｏｒｅ」及び「Ｃｏｐｙ　Ｆｒｅｅ」の４つのステータスを示す。
【０００５】「Ｃｏｐｙ　Ｎｅｖｅｒ」とは、デジタルコンテンツのコピーを全く許さないことを示す。「Ｃｏｐｙ　ｏｎｅ　Ｇｅｎｅｒａｔｉｏｎ」とは、一世代だけデジタルコンテンツのコピーを許すことを示す。コピーされた側のデジタルコンテンツのコピー制御情報は「Ｃｏｐｙ　Ｎｏ　ｍｏｒｅ」となる。
【０００６】「Ｃｏｐｙ　Ｎｏ　ｍｏｒｅ」とは、「Ｃｏｐｙ　ｏｎｅ　Ｇｅｎｅｒａｔｉｏｎ」のデジタルコンテンツからコピーされたデジタルコンテンツに添付されるコピー制御情報であり、以前はコピーを許したが今はコピーを許さないことを示す。「Ｃｏｐｙ　Ｆｒｅｅ」とは、自由にデジタルコンテンツのコピーを許すことを示す。
【０００７】ここでデジタルコンテンツが商用デジタル放送等によって伝送路を介して供給される場合には、コピー制御情報が「Ｃｏｐｙ　Ｎｅｖｅｒ」、「Ｃｏｐｙ　ｏｎｅ　Ｇｅｎｅｒａｔｉｏｎ」及び「Ｃｏｐｙ　Ｎｏ　ｍｏｒｅ」のデジタルコンテンツは必ず暗号化コンテンツの状態で供給され伝送路上における安全が確保される。なお「Ｃｏｐｙ　Ｆｒｅｅ」のデジタルコンテンツは通常、暗号化されない状態で供給される。
【０００８】
【発明が解決しようとする課題】コピー制御情報が「Ｃｏｐｙ　Ｎｅｖｅｒ」であるデジタルコンテンツを伝送路を介して入手して再生する場合や、コピー制御情報が「Ｃｏｐｙ　ｏｎｅ　Ｇｅｎｅｒａｔｉｏｎ」であるデジタルコンテンツを入手して記録媒体に記録することによりコピー制御情報が「Ｃｏｐｙ　Ｎｏ　ｍｏｒｅ」であるデジタルコンテンツが生成される場合等に、これらのデジタルコンテンツのコピーを全く許さないものとするとユーザにとって甚だ利便性が低い事態が考えられる。
【０００９】伝送路を介して供給されるデジタルコンテンツがコピー不可でない場合は、デジタルコンテンツを受信側の記録媒体に記録しておいて後で視聴したり、ＨＤＤ（ハードディスクドライブ）等の記録媒体に記録しながら再生することによりタイムシフト視聴が可能であるが、このデジタルコンテンツのコピーが全く許されない場合は、ユーザは視聴の途中でトイレに行ったり来客や電話等により視聴を中断してしまうと再放送でもない限り視聴を中断した部分を全く視聴できない。例えば、多くの映画は２時間程度が普通であり、４時間を超える長編物も珍しいものではなく、商用デジタル放送等では普通コマーシャルが無いこと等を考えると、コピー制御

情報が「Ｃｏｐｙ　Ｎｅｖｅｒ」であることによりコピーが全く許されないとされた映画等をユーザが全て視聴する為には、２～４時間もの間全くトイレに行く事もできず、来客も電話も許されないなどと言う甚だ利便性が低い事態となってしまう。

【００１０】また、入手し記録媒体に記録したデジタルコンテンツがコピー不可とならない場合は、デジタルコンテンツを他の記録媒体に自由にコピーしたり移動したりすることができるが、このデジタルコンテンツのコピーが全く許されない場合は、ユーザは入手したデジタルコンテンツを一旦どこかの記録媒体に記録してしまうと後で移動することができない。例えば、ＨＤＤ等のアクセス速度が速く使い勝手のよい固定記録媒体を汎用的に使用する方が利便性が高いので、ユーザは入手したデジタルコンテンツをとりあえず固定記録媒体に記録するのが普通であるが、固定記録媒体の記録容量は限られており、またＨＤＤ等の汎用記録媒体は絶えず使用されている等の理由からリムーバルな他の記録媒体に比べて壊れる可能性が高いので、ユーザが一旦視聴する等して長期に保存したいと判断したデジタルコンテンツは、記録容量が限られず保存の面で有利なＤＶＤ－ＲＷやデジタルビデオ等のリムーバルな記録媒体に移動する事が望ましい。

【００１１】とはいえ、ユーザにとっての利便性を向上させる為に、著作権保護要とされコピー不可とされたデジタルコンテンツを勝手にコピー不可でないように変更することは著作権保護の観点から許される事ではない。本来、コピー制御情報が「Ｃｏｐｙ　Ｎｅｖｅｒ」のデジタルコンテンツは、著作権保護の観点から視聴は許すが複製品を禁止することを示し、コピー制御情報が「Ｃｏｐｙ　ｏｎｅ　Ｇｅｎｅｒａｔｉｏｎ」のデジタルコンテンツは、著作権保護の観点から１世代限りの複製品を許すことを示す筈である。

【００１２】そこで、特定の条件の下でのコピーを許す代わりに確実に然るべきデジタルコンテンツを無効化することにより、複製品を許さないという趣旨を逸脱せずにユーザの利便性を向上させることができるものと考える。本発明は、複製品を許さないという趣旨を逸脱せずにユーザの利便性を向上させることができるデータ無効化装置、データ無効化方法、データ無効化プログラム、及び、データ無効化プログラムを記録するコンピュータ読み取り可能な記録媒体を提供することを目的とする。

【００１３】

【課題を解決するための手段】上記目的を達成するために、本発明に係るデータ無効化装置は、一の記録媒体に記録された対象データを無効化するデータ無効化装置であって、前記対象データは複数の部分データから構成され、前記部分データ単位で前記一の記録媒体に記録された対象データを無効化すべきか否か判断する判断手段と、前記判断手段により所定数又は所定量の部分データに対して無効化すべきと判断される度に前記一の記録媒体に記録された対象データのうちの当該無効化すべきと判断された部分データを逐次無効化する逐次無効化手段とを備えることを特徴とする。

【００１４】これによって、対象データを所定数又は所定量の部分データ毎に、所定の条件が満たされた部分データを逐次無効化することができる。従って、対象データの一時的な使用は許すが複製品の生成を禁止したり、１世代限りの複製品を許す等の場合において、禁止された複製品の生成を一時的に許す代わりにその複製品又はオリジナルを無効化することができ、複製品を許さないという趣旨を逸脱せずにユーザの利便性を向上させることができる。

【００１５】また、逐次複製品を無効化するので、悪意ある者が動作の途中で電源を抜くなどの小細工をして複製品を残そうとしても、所定数又は所定量の部分データ分の複製品を残す事が精一杯となるため、この単位を適切に選ぶことによりセキュリティを高めることができる。

【００１６】

【発明の実施の形態】（実施の形態１）

＜概要＞本発明の実施の形態１は、複製品を許さないという趣旨のデジタルコンテンツを受信した場合において、一時的に記録を許すが、再生した場合や予め定めた一定時間を経過した場合には無効化する装置であり、１回限りの視聴、又は、受信から一定時間内に限りタイムシフト視聴を可能とするものである。

【００１７】＜構成＞図１は、本発明の実施の形態１に係る受信再生無効化システムのハードウエア構成の一例を示す図である。ここで図１には、説明の為に、アンテナ９０１、受信装置９０２、モニタ９０３、ＲＡＭ９０４、ＨＤＤ９０５、ＤＶＤレコーダ９０６及びＲＯＭ９０７を記載している。ここで、システムＬＳＩ８００、ＲＡＭ９０４、ＨＤＤ９０５及びＲＯＭ９０７は通常、ＳＴＢ（Ｓｅｔ　Ｔｏｐ　Ｂｏｘ）と呼ばれる同一筐体内に収納されている。

【００１８】図１に示すシステムＬＳＩ８００は、トランスポートストリームデコーダ８０１、ＡＶデコーダ８０２、暗号エンジン８０３及びマイコン８０４からなり、これらを同一の半導体チップ内に収めることにより、トランスポートストリームをデコードした直後の何の暗号化もされていないデジタルデータを回路基盤の配線上に出さないようにしてセキュリティの強化を図っている。

【００１９】受信装置９０２は、アンテナ９０１を介して放送局から所望の搬送波を受信して復調し、利用すべきデジタルコンテンツや制御データのパケットからなるトランスポートストリーム（以下「ＴＳストリーム」という）を生成する。ここでは、利用すべきデジタルコンテンツが著作権保護要の場合には、例えばデジタルコン

テンツに添付されたコピー制御情報が「Ｃｏｐｙ　Ｎｅｖｅｒ」とされることなどによって複製品を許さないという趣旨の情報がデジタルコンテンツに添付され、さらにＴＳストリームのうち、制御情報等であるヘッダ部はそのままであるが、送信すべきデータであるペイロード部がスクランブルと呼ばれる暗号方式により暗号化される。

【００２０】トランスポートストリームデコーダ８０１は、受信装置９０２により生成されたＴＳストリームを、スクランブルされているものに対しては予め正当なユーザに与えられる復号鍵を用いて復号（デスクランブル）してデコードし、スクランブルされていないものに対してはそのままデコードし、利用すべきデジタルコンテンツを生成する。例えばここで生成される利用すべきデジタルコンテンツは、音声及び画像のＭＰＥＧストリームである。

【００２１】ＡＶデコーダ８０２は、トランスポートストリームデコーダ８０１により生成されたデジタルコンテンツから映像出力信号及び音声出力信号を生成しモニタ９０３に映像及び音声を再生させる。暗号エンジン８０３は、利用すべきデジタルコンテンツが著作権保護要の場合であって、ＲＡＭ９０４、ＨＤＤ９０５及びＤＶＤレコーダ９０６等の記録媒体に記録が必要な場合に、トランスポートストリームデコーダ８０１により生成された利用すべきデジタルコンテンツを、所定の再生時間に相当する分毎に、ここでランダムに生成した暗号鍵を用いて暗号化し、対応する復号鍵をデバイスＩＤを用いて暗号化してセットで記録し、デジタルコンテンツを使用する際には、暗号化された復号鍵をデバイスＩＤを用いて復号し、これを用いて暗号化されたデジタルコンテンツを復号する。ここでデバイスＩＤとは、半導体チップ毎に固有の値であり、ここでは半導体チップの外部からは参照できないものとする。

【００２２】マイコン８０４は、ＲＯＭ９０７に記録された制御プログラムを読み出して実行することにより、ＳＴＤ全体の動作を制御する。ここでは制御プログラムが悪意のあるユーザに勝手に書き換えられないようにスクランブルされているものとし、デスクランブルしてから実行されるものとする。ここでユーザが、複製品を許さないという趣旨の情報が添付されたデジタルコンテンツを視聴している途中で、なんらかの所用の為にタイムシフト視聴を指示したとすると、マイコン８０４は暗号化させたデジタルコンテンツをＨＤＤ９０５に記録させ続けながら、シフト時間の分だけ前の、ＨＤＤ９０５に記録された暗号化されたデジタルコンテンツを復号させて再生させ続けると同時に、再生されたデジタルコンテンツに対応するＨＤＤ９０５内の暗号化されたデジタルコンテンツを、所定の再生時間の分毎に、再生できないように順次無効化する。

【００２３】ここでは、暗号化されたデジタルコンテンツを再生されたことを条件に無効化したが、単に、又は、さらに、記録してから所定の時間が経過したことを条件に無効化してもよい。多くの映画は２時間程度が普通なので、この所定の時間を例えば９０分程度に設定しておけば、多くの映画が記録媒体に丸々記録された状態に一瞬たりともなり得ず、処理の途中で電源を切る等しても映画の１本分も残せない。よって、後々映画の１本分を再生することはできないことになり、この所定の時間の分だけに限りタイムシフト視聴を許すことができる。

【００２４】図２は、本発明の実施の形態１に係る受信再生無効化装置の機能ブロック図である。図２に示す受信再生無効化装置１００は、ユーザインタフェイス部１０１、受信部１０２、デスクランブル部１０３、個別鍵生成部１０４、データ暗号化部１０５、鍵暗号化部１０６、記録部１０７、鍵復号部１０８、データ復号部１０９、再生部１１０、無効化判断部１１１、処理能力判断部１１２、逐次無効化部１１３、完全無効化部１１４を備える。ここで実際には、受信部１０２の機能は図１の受信装置９０２の機能に相当し、デスクランブル部１０３の機能は図１のトランスポートストリームデコーダ８０１の機能に相当し、個別鍵生成部１０４、データ暗号化部１０５、鍵暗号化部１０６、記録部１０７、鍵復号部１０８、データ復号部１０９の機能は図１の暗号エンジン８０３の機能に相当し、再生部１１０はの機能は図１のＡＶデコーダ８０２の機能に相当し、無効化判断部１１１、処理能力判断部１１２、逐次無効化部１１３、完全無効化部１１４の機能は図１のマイコン８０４の機能に相当する。

【００２５】なお、説明を容易にするために発明と直接関係ない機能の説明は省略しているので、実際のものとは多少異なる。ユーザインタフェイス部１０１は、ユーザから視聴指示、一時停止指示、タイムシフト視聴指示、停止指示、及び、デジタルコンテンツの移動指示等の各種の指示を受け付ける。

【００２６】受信部１０２は、放送局等から放送される送信データを受信する。ここでは、コピー制御情報が添付されスクランブルされたデジタルコンテンツを受信するものとする。デスクランブル部１０３は、受信部１０２により受信されたスクランブルされたデジタルコンテンツを、予め正当なユーザに与えられる復号鍵を用いてデスクランブルする。

【００２７】個別鍵生成部１０４は、ユーザが一時停止指示をしている間に、所定の放送時間に相当するデジタルコンテンツ毎に、乱数等を用いて任意の暗号鍵とこれに対応する復号鍵との組をランダムに生成する。ここでは、復号鍵と暗号鍵とが同一となるようなアルゴリズムを用いることとし、以下、復号鍵及び暗号鍵を共に生成鍵と呼ぶ。例えば１０分の放送時間に相当するデジタルコンテンツ毎に、対応する生成鍵をランダムに生成す

る。

【００２８】データ暗号化部１０５は、ユーザが一時停止指示をしている間に、デスクランブル部１０３によりデスクランブルされたデジタルコンテンツを、所定の放送時間に相当する分毎に、個別鍵生成部１０４により生成された暗号鍵を用いて、対応する復号鍵によって復号可能なように暗号化する。ここでは、１０分の放送時間に相当するデジタルコンテンツを対応する生成鍵を用いて暗号化する。

【００２９】鍵暗号化部１０６は、データ暗号化部１０５により暗号化に用いられた暗号鍵に対応する復号鍵を、デバイスＩＤを用いて暗号化する。ここでは、デバイスＩＤを用いて対応する生成鍵を暗号化する。記録部１０７は、データ暗号化部１０５により暗号化された所定の放送時間に相当するデジタルコンテンツと鍵暗号化部１０６により暗号化された対応する復号鍵との組を順次所定の記録媒体に記録する。ここでは、生成鍵を用いて暗号化された１０分の放送時間に相当するデジタルコンテンツと暗号化された当該生成鍵との組を順次ＨＤＤに記録する。なお、デジタルコンテンツは、著作権保護不要の場合には暗号化せずに記録してもよい。

【００３０】鍵復号部１０８は、ユーザがタイムシフト視聴指示をしている間に、再生すべきデジタルコンテンツに対応する暗号化された復号鍵を、先に記録された記録媒体から読み出してデバイスＩＤを用いて復号する。ここでは、シフト時間の分だけ前のデジタルコンテンツと組になっている暗号化された生成鍵を復号する。データ復号部１０９は、ユーザがタイムシフト視聴指示をしている間に、鍵復号部１０８により復号された復号鍵を用いて、再生すべきデジタルコンテンツを復号する。ここでは、復号された生成鍵を用いて、シフト時間の分だけ前のデジタルコンテンツを復号する。

【００３１】再生部１１０は、ユーザが視聴指示をしている間はデスクランブル部１０３によりデスクランブルされたデジタルコンテンツを再生し、ユーザがタイムシフト視聴指示をしている間は、データ復号部１０９により復号されたデジタルコンテンツを再生する。無効化判断部１１１は、複製品の生成を禁止されたデジタルコンテンツであるのもかかわらず受信されて一時記録された組を対象として、所定の放送時間に相当する単位で、先に記録媒体に記録された組を、所定の条件に基づいて無効化すべきか否かを判断する。ここでは、１０分の放送時間に相当する暗号化されたデジタルコンテンツと暗号化された生成鍵との組単位で、無効化すべきか否かを判断する。

【００３２】ここで、無効化判断部１１１による無効化すべき判断の条件は、再生部１１０により再生された事や、受信部１０２により受信されてから又は記録部１０７により記録されてから所定時間が経過した事である。なお、所定時間が経過した事をもって無効化すべきと判断する場合には、記録部１０７はさらに、記録期限を管理するために所定の放送時間に相当するデジタルコンテンツの受信時刻や記録時刻等の期限管理情報を記録し、無効化判断部１１１はこの期限管理情報に基づいて記録期限が切れたか否かを判断する。

【００３３】処理能力判断部１１２は、無効化すべきと判断されたデジタルコンテンツに関わるデータを全て逐次破壊するだけの処理能力の余裕が有るか否かを判断する。逐次無効化部１１３は、所定数又は所定量のデジタルコンテンツと復号鍵とが無効化すべきと判断される度に、先に記録されたうちの無効化すべきと判断された部分を逐次無効化する。

【００３４】ここで逐次無効化部１１３による無効化とは、記録媒体上のデータを使用不能にすることを意味する。一般のデータ消去は、データファイルのリンク情報のみを消去したりデータファイルのヘッダ部分の数ビットのみを書き換えるだけで、データ部分がそっくそのまま残っているのが普通であり、消去指示後にデータを復帰できる場合もあるので、このようなデータ消去ではデータを使用不能にしたとは言えない。従って、逐次無効化部１１３は記録媒体上の無効化すべきデータが記録されている記録領域に任意のデータを上書きしたり、その記録領域を初期化するなどしてデータそのものを破壊する。

【００３５】ここで、逐次無効化部１１３は無効化すべきデータの全てを逐次破壊してもよいのだが、実際には、無効化すべきデータと同じサイズの任意のデータを逐次上書きすると装置自体の処理能力が問題となる場合がある。例えばタイムシフト視聴を実行している時は、放送されるデジタルコンテンツを受信し、デスクランブルし、暗号化し、記録するといった一連の処理と、記録されたデジタルコンテンツを読み出し、復号し、再生するといった一連の処理を同時にこなす必要があり、制御系及び記録媒体等の負荷が大きい。このようにただでさえ負荷の大きな処理であるところに、さらに、無効化すべきデータの全てと同じサイズの任意のデータを逐次上書きするといった負荷の大きな処理を同時に実行するとなると、装置自体の処理能力を高くするか、他の機能を制限することになる。

【００３６】しかし、データを無効化すること自体がユーザに何の利益を与えるものでもないので、処理能力を高くすることでコストアップしたり、他の機能が制限されるような事態は避けたい。そこで逐次無効化部１１３は、少なくとも重要な部分を逐次破壊することとする。ここで重要な部分とは、例えば再生する際に他のデータを再生するために先に必要となるデータであり、具体的には復号鍵であり、ＭＰＥＧデータにおけるＩピクチャーであり、Ｉピクチャーの先頭のセクタである。

【００３７】また、逐次無効化部１１３は、処理能力判断部１１２により処理能力の余裕があると判断された場

合に無効化すべきデータを全て破壊し、処理能力の余裕がないと判断された場合に先に必要となるデータのみを破壊することとしてもよい。完全無効化部１１４は、無効化すべきデータのうち、逐次無効化部１１３により逐次破壊されなかった部分のデータを、処理能力に余裕がある時に全て破壊する。また、ユーザがタイムシフト視聴を止める指示をした場合には、破壊されずに残っているデータを全て破壊する。

【００３８】＜動作１＞図３は、本発明の実施の形態１に係る受信再生無効化装置の動作の一例を示す図である。以下に図３を用いて、本発明の逐次再生、蓄積、タイムシフト、及び、無効化の動作を説明する。

【００３９】（１）停止状態において、ユーザインタフェイス部１０１が何らかの番組の視聴指示をユーザから受け付けるまで待つ（ステップＳ１）。

（２）視聴指示を受け付けると（ステップＳ１：Ｙｅｓ）逐次再生動作を開始する（ステップＳ２）。

受信部１０２が、ユーザにより視聴指示された番組の送信データの受信を開始する。ここでは、コピー制御情報「Ｃｏｐｙ　Ｎｅｖｅｒ」が添付されスクランブルされたデジタルコンテンツの受信を開始するものとする。

【００４０】デスクランブル部１０３が、受信部１０２により受信が開始されたスクランブルされたデジタルコンテンツのデスクランブルを開始する。再生部１１０が、デスクランブル部１０３によりデスクランブルされたデジタルコンテンツの逐次再生を開始する。

（３）逐次再生動作中において、ユーザインタフェイス部１０１が停止指示をユーザから受け付けるまで待つ（ステップＳ３）。

【００４１】（４）停止指示を受け付けると（ステップＳ３：Ｙｅｓ）、受信部１０２、デスクランブル部１０３、再生部１１０の各処理を停止して逐次再生動作を終了し停止状態に戻る（ステップＳ４）。

（５）逐次再生動作中において、ユーザインタフェイス部１０１が一時停止指示をユーザから受け付けるまで待つ（ステップＳ５）。

【００４２】（６）一時停止指示を受け付けると（ステップＳ５：Ｙｅｓ）、蓄積動作を開始する（ステップＳ６）。

個別鍵生成部１０４が、所定の放送時間に相当するデジタルコンテンツ毎に、乱数等を用いて任意の暗号鍵とこれに対応する復号鍵との組をランダムに生成する。ここでは、１０分の放送時間に相当するデジタルコンテンツ毎に、生成鍵をランダムに生成する。

【００４３】データ暗号化部１０５が、デスクランブル部１０３によりデスクランブルされたデジタルコンテンツを、所定の放送時間に相当する分毎に、個別鍵生成部１０４により生成された暗号鍵を用いて、対応する復号鍵によって復号可能なように暗号化する。ここでは、１０分の放送時間に相当するデジタルコンテンツを対応する生成鍵を用いて暗号化する。

【００４４】鍵暗号化部１０６が、データ暗号化部１０５により暗号化に用いられた暗号鍵に対応する復号鍵を、デバイスＩＤを用いて暗号化する。ここでは、デバイスＩＤを用いて対応する生成鍵を暗号化する。記録部１０７が、データ暗号化部１０５により暗号化された所定の放送時間に相当するデジタルコンテンツと、鍵暗号化部１０６により暗号化された対応する復号鍵とを記録媒体に記録する。ここでは、生成鍵を用いて暗号化された１０分の放送時間に相当するデジタルコンテンツと暗号化された当該生成鍵との組をＨＤＤに記録する。

【００４５】再生部１１０によるデジタルコンテンツの逐次再生を止める。

（７）蓄積動作中において、無効化判断部１１１が、所定の放送時間に相当する単位で、先に記録媒体に記録された暗号化されたデジタルコンテンツと暗号化された復号鍵との組の中で記録期限が切れた組が有るか否かを判断する。ここでは、記録期限を記録から９０分とし、１０分の放送時間に相当する単位で、記録してから９０分を経過した組を記録期限が切れた組と判断する（ステップＳ７）。

【００４６】（８）記録期限が切れた組がある場合には、逐次無効化部１１３がその都度、記録期限が切れた組中の暗号化された復号鍵が記録された記録領域に任意のデータを上書きして、当該記録領域のデータを逐次無効化する。ここで、処理能力判断部１１２が、処理能力の余裕が有ると判断した場合には、さらに、記録期限が切れた組中の暗号化されたデジタルコンテンツに任意のデータを上書きして、当該記録領域のデータを逐次無効化する（ステップＳ８）。

【００４７】（９）蓄積動作中において、ユーザインタフェイス部１０１が停止指示をユーザから受け付けるまで待つ（ステップＳ９）。

（１０）停止指示を受け付けると（ステップＳ９：Ｙｅｓ）、受信部１０２、デスクランブル部１０３、個別鍵生成部１０４、データ暗号化部１０５、鍵暗号化部１０６、記録部１０７の各処理を停止して蓄積動作を終了し、完全無効化部１１４が、破壊されずに残っているデータを全て破壊して停止状態に戻る（ステップＳ１０）。

【００４８】（１１）蓄積動作中において、ユーザインタフェイス部１０１がタイムシフト視聴指示をユーザから受け付けるまで待つ（ステップＳ１１）。

（１２）タイムシフト視聴指示を受け付けると（ステップＳ１１：Ｙｅｓ）、タイムシフト動作を開始する（ステップＳ１２）。

鍵復号部１０８が、先に記録された記録媒体から、シフト時間の分だけ前のデジタルコンテンツと組になっている暗号化された復号鍵を読み出して、デバイスＩＤを用いて復号する。ここでは、シフト時間を３０分とし、３

０分～２０分前の１０分間に相当するデジタルコンテンツと組になっている暗号化された生成鍵から復号を開始する。なお、シフト時間が記録期限を越える場合には、シフト時間の分だけ前の組は既に無効化されているので再生できないため、この場合のシフト時間を記録期限として動作を続行する。

【００４９】データ復号部１０９が、鍵復号部１０８により復号された復号鍵を用いて、対応するデジタルコンテンツの復号を開始する。ここでは、復号された生成鍵を用いて、３０分～２０分前の１０分間に相当するデジタルコンテンツから復号を開始する。再生部１１０が、データ復号部１０９により復号されたデジタルコンテンツの再生を開始する。

【００５０】（１３）タイムシフト動作中において、無効化判断部１１１が、所定の放送時間に相当する単位で、先に記録媒体に記録された暗号化されたデジタルコンテンツと暗号化された復号鍵との組の中で記録期限が切れたか、又は、再生部１１０により再生されたデジタルコンテンツに対応する組が有るか否かを判断する。ここでは、記録期限を９０分とし、１０分の放送時間に相当する単位で、記録してから９０分を経過した、又は、再生されたデジタルコンテンツを無効化すべき組と判断する（ステップＳ１３）。

【００５１】（１４）無効化すべき組がある場合には、逐次無効化部１１３がその都度、無効化すべき組中の暗号化された復号鍵が記録された記録領域に任意のデータを上書きして、当該記録領域のデータを逐次無効化する。ここで、処理能力判断部１１２が、処理能力の余裕が有ると判断した場合には、さらに、無効化すべき組中の暗号化されたデジタルコンテンツに任意のデータを上書きして、当該記録領域のデータを逐次無効化する（ステップＳ１４）。

【００５２】（１５）タイムシフト動作中において、ユーザインタフェイス部１０１が停止指示をユーザから受け付けるまで待つ（ステップＳ１５）。

（１６）停止指示を受け付けると（ステップＳ１５：Ｙｅｓ）、受信部１０２、デスクランブル部１０３、個別鍵生成部１０４、データ暗号化部１０５、鍵暗号化部１０６、記録部１０７、鍵復号部１０８、データ復号部１０９、再生部１１０の各処理を停止してタイムシフト動作を終了し、完全無効化部１１４が、破壊されずに残っているデータを全て破壊して停止状態に戻る（ステップＳ１６）。

【００５３】（１７）タイムシフト動作中において、ユーザインタフェイス部１０１が一時停止指示をユーザから受け付けるまで待つ（ステップＳ１７）。

（１８）一時停止指示を受け付けると（ステップＳ１７：Ｙｅｓ）、鍵復号部１０８、データ復号部１０９、再生部１１０の各処理を停止して蓄積動作に移行する（ステップＳ１８）。

【００５４】＜動作２＞動作１では、逐次再生動作中は蓄積動作は行わなず、一時停止指示をユーザから受け付けた場合に逐次再生動作を止めて蓄積動作に移行したが、動作２では、逐次再生動作中において蓄積動作を同時に行い、ユーザが一時停止を指示していなくてもタイムシフト視聴指示を可能にし、さらに、一時停止時間が上限に達すると自動的に一時停止を解除してタイムシフト動作に移行する自動一時停止解除機能を追加するものである。

【００５５】図４は、本発明の実施の形態１に係る受信再生無効化装置の動作の別の例を示す図である。なお、受信部１０２により受信されるデジタルコンテンツには、記録期限（Storage Time）と再視聴期限（View TIme）とが添付されているものとする。ここで、記録期限とは各組毎に記録されてから記録が許されるまでの時間を、再視聴期限とは各組毎に最初に再生されてから再視聴が許されるまでの時間を示し、記録期限と再視聴期限のどちらか一方でも経過した組を無効化すべき対象とする。

【００５６】以下に図４を用いて、本発明の逐次再生蓄積、蓄積、タイムシフト、無効化、及び、自動一時停止解除の動作を説明する。なお、実施の形態１と同様の動作ステップには同じ番号を付す。

（１）停止状態において、ユーザインタフェイス部１０１が何らかの番組の視聴指示をユーザから受け付けるまで待つ（ステップＳ１）。

【００５７】（２）視聴指示を受け付けると（ステップＳ１：Ｙｅｓ）逐次再生蓄積動作を開始する（ステップＳ１０２）。

受信部１０２が、ユーザにより視聴指示された番組の送信データの受信を開始する。ここでは、コピー制御情報「Ｃｏｐｙ　Ｎｅｖｅｒ」が添付されスクランブルされたデジタルコンテンツの受信を開始するものとする。

【００５８】デスクランブル部１０３が、受信部１０２により受信が開始されたスクランブルされたデジタルコンテンツのデスクランブルを開始する。再生部１１０が、デスクランブル部１０３によりデスクランブルされたデジタルコンテンツの逐次再生を開始する。個別鍵生成部１０４が、所定の放送時間に相当するデジタルコンテンツ毎に、乱数等を用いて任意の暗号鍵とこれに対応する復号鍵との組をランダムに生成する。ここでは、１０分の放送時間に相当するデジタルコンテンツ毎に、生成鍵をランダムに生成する。

【００５９】データ暗号化部１０５が、デスクランブル部１０３によりデスクランブルされたデジタルコンテンツを、所定の放送時間に相当する分毎に、個別鍵生成部１０４により生成された暗号鍵を用いて、対応する復号鍵によって復号可能なように暗号化する。ここでは、１０分の放送時間に相当するデジタルコンテンツを対応する生成鍵を用いて暗号化する。

【００６０】鍵暗号化部１０６が、データ暗号化部１０５により暗号化に用いられた暗号鍵に対応する復号鍵を、デバイスＩＤを用いて暗号化する。ここでは、デバイスＩＤを用いて対応する生成鍵を暗号化する。記録部１０７が、データ暗号化部１０５により暗号化された所定の放送時間に相当するデジタルコンテンツと、鍵暗号化部１０６により暗号化された対応する復号鍵とを記録媒体に記録する。ここでは、生成鍵を用いて暗号化された１０分の放送時間に相当するデジタルコンテンツと暗号化された当該生成鍵との組をＨＤＤに記録する。

【００６１】ここで、記録媒体に記録されるそれぞれの組には期限管理情報とともに記録期限と再視聴期限とが添付され、一度再生された組には最初の再生時刻が期限管理情報に付加されるものとする。

（３）逐次再生蓄積動作中において、無効化判断部１１１が期限管理情報を参照して、所定の放送時間に相当する単位で、先に記録媒体に記録された暗号化されたデジタルコンテンツと暗号化された復号鍵との組の中で、記録期限が切れた組が有るか否かを判断し、さらに、再生された組に対しては、再視聴期限が切れた組が有るか否かを判断する。ここでは、記録期限を記録から９０分、再視聴期限を再生から６０分とし、１０分の放送時間に相当する単位で、記録してから９０分を経過した組を記録期限が切れた組と判断し、さらに、視聴から６０分を経過した組を再視聴期限が切れた組と判断する（ステップＳ１０３）。

【００６２】（４）記録期限又は再視聴期限が切れた組がある場合には、逐次無効化部１１３がその都度、記録期限又は再視聴期限が切れた組中の暗号化された復号鍵が記録された記録領域に任意のデータを上書きして、当該記録領域のデータを逐次無効化する。ここで、処理能力判断部１１２が、処理能力の余裕が有ると判断した場合には、さらに、記録期限又は再視聴期限が切れた組中の暗号化されたデジタルコンテンツに任意のデータを上書きして、当該記録領域のデータを逐次無効化する（ステップＳ１０４）。

【００６３】（５）逐次再生蓄積動作中において、ユーザインタフェイス部１０１が停止指示をユーザから受け付けるまで待つ（ステップＳ１０５）。

（６）停止指示を受け付けると（ステップＳ１０５：Ｙｅｓ）、受信部１０２、デスクランブル部１０３、再生部１１０、個別鍵生成部１０４、データ暗号化部１０５、鍵暗号化部１０６、記録部１０７の各処理を停止して逐次再生蓄積動作を終了し、完全無効化部１１４が、破壊されずに残っているデータを全て破壊して停止状態に戻る（ステップＳ１０６）。

【００６４】（７）逐次再生蓄積動作中において、ユーザインタフェイス部１０１がタイムシフト視聴指示をユーザから受け付けるまで待つ（ステップＳ１０７）。

（８）逐次再生蓄積動作中において、ユーザインタフェイス部１０１が一時停止指示をユーザから受け付けるまで待つ（ステップＳ１０８）。

（９）一時停止指示を受け付けると（ステップＳ１０８：Ｙｅｓ）、再生動作を終了し、蓄積動作を継続する（ステップＳ１０９）。

【００６５】再生部１１０によるデジタルコンテンツの逐次再生を止める。

（１０）蓄積動作中において、無効化判断部１１１が期限管理情報を参照して、所定の放送時間に相当する単位で、先に記録媒体に記録された暗号化されたデジタルコンテンツと暗号化された復号鍵との組の中で、記録期限が切れた組が有るか否かを判断し、さらに、再生された組に対しては、再視聴期限が切れた組が有るか否かを判断する（ステップＳ１１０）。

【００６６】（１１）記録期限又は再視聴期限が切れた組がある場合には、逐次無効化部１１３がその都度、記録期限又は再視聴期限が切れた組中の暗号化された復号鍵が記録された記録領域に任意のデータを上書きして、当該記録領域のデータを逐次無効化する。ここで、処理能力判断部１１２が、処理能力の余裕が有ると判断した場合には、さらに、記録期限又は再視聴期限が切れた組中の暗号化されたデジタルコンテンツに任意のデータを上書きして、当該記録領域のデータを逐次無効化する（ステップＳ１１１）。

【００６７】（１２）蓄積動作中において、ユーザインタフェイス部１０１が停止指示をユーザから受け付けるまで待つ（ステップＳ９）。

（１３）停止指示を受け付けると（ステップＳ９：Ｙｅｓ）、受信部１０２、デスクランブル部１０３、個別鍵生成部１０４、データ暗号化部１０５、鍵暗号化部１０６、記録部１０７の各処理を停止して蓄積動作を終了し、完全無効化部１１４が、破壊されずに残っているデータを全て破壊して停止状態に戻る（ステップＳ１０）。

【００６８】（１４）蓄積動作中において、ユーザインタフェイス部１０１がタイムシフト視聴指示をユーザから受け付けるまで待つ（ステップＳ１１）。

（１５）蓄積動作中において、逐次無効化部１１３がシフト時間が上限値に達しているか否かを判断する。上限値に達している場合はシフト時間を上限値に設定して自動的に一時停止を解除してタイムシフト動作へ移行する（ステップＳ１１５）。ここでは、シフト時間の上限値を記録期限と同じ９０分とし、これによって一度も再生されないまま記録期限が切れることにより無効化されるデータをなくすことができる。

【００６９】（１６）自動一時停止解除の場合（ステップＳ１１５：Ｙｅｓ）、又は、タイムシフト視聴指示を受け付けると（ステップＳ１０７：ＹｅｓステップＳ１１：Ｙｅｓ）、タイムシフト動作を開始する（ステップＳ１１６）。

鍵復号部１０８が、先に記録された記録媒体から、シフト時間の分だけ前のデジタルコンテンツと組になっている暗号化された復号鍵を読み出して、デバイスＩＤを用いて復号する。ここでは、シフト時間を３０分とし、３０分～２０分前の１０分間に相当するデジタルコンテンツと組になっている暗号化された生成鍵から復号を開始する。なお、シフト時間が記録期限を越える場合には、シフト時間の分だけ前の組は既に無効化されているので再生できないため、この場合のシフト時間を記録期限として動作を続行する。

【００７０】データ復号部１０９が、鍵復号部１０８により復号された復号鍵を用いて、対応するデジタルコンテンツの復号を開始する。ここでは、復号された生成鍵を用いて、３０分～２０分前の１０分間に相当するデジタルコンテンツから復号を開始する。再生部１１０が、データ復号部１０９により復号されたデジタルコンテンツの再生を開始する。

【００７１】（１７）タイムシフト動作中において、無効化判断部１１１が期限管理情報を参照して、所定の放送時間に相当する単位で、先に記録媒体に記録された暗号化されたデジタルコンテンツと暗号化された復号鍵との組の中で、記録期限が切れた組が有るか否かを判断し、さらに、再生された組に対しては、再視聴期限が切れた組が有るか否かを判断する（ステップＳ１１７）。

【００７２】（１８）記録期限又は再視聴期限が切れた組がある場合には、逐次無効化部１１３がその都度、記録期限又は再視聴期限が切れた組中の暗号化された復号鍵が記録された記録領域に任意のデータを上書きして、当該記録領域のデータを逐次無効化する。ここで、処理能力判断部１１２が、処理能力の余裕が有ると判断した場合には、さらに、記録期限又は再視聴期限が切れた組中の暗号化されたデジタルコンテンツに任意のデータを上書きして、当該記録領域のデータを逐次無効化する（ステップＳ１１８）。

【００７３】（１９）タイムシフト動作中において、ユーザインタフェイス部１０１が停止指示をユーザから受け付けるまで待つ（ステップＳ１５）。

（２０）停止指示を受け付けると（ステップＳ１５：Ｙｅｓ）、受信部１０２、デスクランブル部１０３、個別鍵生成部１０４、データ暗号化部１０５、鍵暗号化部１０６、記録部１０７、鍵復号部１０８、データ復号部１０９、再生部１１０の各処理を停止してタイムシフト動作を終了し、完全無効化部１１４が、破壊されずに残っているデータを全て破壊して停止状態に戻る（ステップＳ１６）。

【００７４】（２１）タイムシフト動作中において、ユーザインタフェイス部１０１が一時停止指示をユーザから受け付けるまで待つ（ステップＳ１７）。

（２２）一時停止指示を受け付けると（ステップＳ１７：Ｙｅｓ）、鍵復号部１０８、データ復号部１０９、再生部１１０の各処理を停止して蓄積動作に移行する（ステップＳ１８）。

【００７５】以上のように、本発明の実施の形態１によれば、複製品の生成が禁止されたデジタルコンテンツに対して、一時記録してタイムシフト視聴を許しながらも、記録物を逐次無効化することができるので、複製品を許さないという趣旨を逸脱せずにユーザの利便性を向上させることができる。

（実施の形態２）

＜概要＞本発明の実施の形態２は、複製品を許さないという趣旨のデジタルコンテンツを受信した場合において、一時的に記録を許すが、一定時間を経過した場合には無効化する装置であり、無効化すべきデジタルコンテンツが記録された記録領域に新しいデジタルコンテンツを順次上書きすることによって、処理能力に影響を与えずに一定時間を経過したデジタルコンテンツを無効化する装置であり、受信から一定時間内に限りタイムシフト視聴を可能とするものである。

【００７６】＜構成＞本発明の実施の形態２に係る受信再生無効化装置のハードウエア構成は、実施の形態１と同様である。図５は、本発明の実施の形態２に係る受信再生無効化装置の機能ブロック図である。

【００７７】図５に示す受信再生無効化装置２００は、ユーザインタフェイス部１０１、受信部１０２、デスクランブル部１０３、個別鍵生成部１０４、データ暗号化部１０５、鍵暗号化部１０６、記録部２０１、鍵復号部１０８、データ復号部１０９、再生部１１０、無効化判断部２０２、処理能力判断部１１２、逐次無効化部２０３、完全無効化部２０４を備える。ここで実際には、受信部１０２の機能は図１の受信装置９０２の機能に相当し、デスクランブル部１０３の機能は図１のトランスポートストリームデコーダ８０１の機能に相当し、個別鍵生成部１０４、データ暗号化部１０５、鍵暗号化部１０６、記録部２０１、鍵復号部１０８、データ復号部１０９の機能は図１の暗号エンジン８０３の機能に相当し、再生部１１０はの機能は図１のＡＶデコーダ８０２の機能に相当し、無効化判断部２０２、処理能力判断部１１２、逐次無効化部２０３、完全無効化部２０４の機能は図１のマイコン８０４の機能に相当する。

【００７８】なお、実施の形態１と同様の構成要素には同じ番号を付し、その説明を省略する。記録部２０１は、データ暗号化部１０５により暗号化された所定の放送時間に相当するデジタルコンテンツと鍵暗号化部１０６により暗号化された対応する復号鍵との組を順次所定の記録媒体に記録するが、複製品の生成を禁止されたデジタルコンテンツを記録する場合には、記録媒体上に、所定の放送時間に相当するデータを記録できる容量の記録領域を複数確保し、確保した記録領域に対して順番に、データ暗号化部１０５により暗号化された所定の放送時間に相当するデジタルコンテンツと鍵暗号化部１０

６により暗号化された対応する復号鍵との組を記録する。ここでは、１０分の放送時間に相当するデータを記録できる容量の記録領域をＨＤＤ上に９個確保し、９個確保した記録領域に対して順番に、生成鍵を用いて暗号化された１０分の放送時間に相当するデジタルコンテンツと暗号化された当該生成鍵との組を記録する。この時、先に記録された組が有る場合には、データを上書きする。なお、デジタルコンテンツは、著作権保護不要の場合には暗号化せずに記録してもよい。

【００７９】無効化判断部２０２は、複製品の生成を禁止されたデジタルコンテンツであるのもかかわらず受信されて一時記録された組を対象として、所定の放送時間に相当する単位で、先に記録媒体に記録された組を、所定の条件に基づいて無効化すべきか否かを判断する。ここでは、１０分の放送時間に相当する暗号化されたデジタルコンテンツと暗号化された生成鍵との組単位で、無効化すべきか否かを判断する。

【００８０】ここで、無効化判断部２０２による無効化すべき判断の条件は、再生部１１０により再生された事や、受信部１０２により受信されてから又は記録部２０１により記録されてから所定時間が経過した事である。ここでは、記録媒体に記録された各組の記録順序を示す順序情報を記録しておき、先に記録された組から順番に無効化すべきと判断し、記録部２０１が無効化すべきと判断された組が記録された記録領域に新しい組を上書きすることにより、記録媒体上に９個確保した記録領域のそれぞれに書き込まれた１０分の放送時間に相当する組は、それぞれ９０分後に新しい組のデータが上書きされることにより無効化される。

【００８１】逐次無効化部２０３は、所定数又は所定量のデジタルコンテンツと復号鍵とが無効化すべきと判断される度に、先に記録されたうちの無効化すべきと判断された部分を逐次無効化する。ここでは、新しい組のデータを記録している間は、記録すると同時に逐次無効化することができ、新しい組のデータを記録しなくなった場合には、記録媒体上の無効化すべきデータが記録されている記録領域に継続的に任意のデータを上書きするなどしてデータそのものを破壊する。

【００８２】ここで、記録すべきデータが、時間あたりのデータ量が一定であるような固定ビットレートである場合には、無効化すべきデータが新しいデータの上書きによって全て無効化されるが、ＭＰＥＧのように可変ビットレートである場合には無効化すべきデータが新しいデータの上書きによって全て無効化されないことがある。

【００８３】そこで、逐次無効化部２０３は新しいデータの上書きによって無効化されなかった部分に意味のないデータを上書きするなどして、無効化すべきデータの全てを逐次破壊してもよいのだが、処理能力判断部１１２により処理能力の余裕があると判断された場合に無効化すべきデータを全て破壊し、処理能力の余裕がないと判断された場合には新しいデータの上書きによって無効化されなかった部分をそのままにすることとしてもよい。

【００８４】完全無効化部２０４は、無効化すべきデータのうち、逐次無効化部２０３により逐次破壊されなかった部分のデータを、処理能力に余裕がある時に全て破壊する。また、ユーザがタイムシフト視聴を止める指示をした場合には、破壊されずに残っているデータを全て破壊する。

＜動作＞図６は、本発明の実施の形態２に係る受信再生無効化装置の動作の一例を示す図である。

【００８５】以下に図６を用いて、本発明の逐次再生、蓄積、タイムシフト、及び、無効化の動作を説明する。なお、実施の形態１と同様の動作ステップには同じ番号を付し、その説明を省略する。（１）～（５）実施の形態１の図３の（１）～（５）に同じ（ステップＳ１～Ｓ５）。

（６）一時視聴停止指示を受け付けると（ステップＳ５：Ｙｅｓ）、蓄積動作を開始する（ステップＳ２１）。

【００８６】個別鍵生成部１０４が、所定の放送時間に相当するデジタルコンテンツ毎に、乱数等を用いて任意の暗号鍵とこれに対応する復号鍵との組をランダムに生成する。ここでは、１０分の放送時間に相当するデジタルコンテンツ毎に、生成鍵をランダムに生成する。データ暗号化部１０５が、デスクランブル部１０３によりデスクランブルされたデジタルコンテンツを、所定の放送時間に相当する分毎に、個別鍵生成部１０４により生成された暗号鍵を用いて、対応する復号鍵によって復号可能なように暗号化する。ここでは、１０分の放送時間に相当するデジタルコンテンツを対応する生成鍵を用いて暗号化する。

【００８７】鍵暗号化部１０６が、データ暗号化部１０５により暗号化に用いられた暗号鍵に対応する復号鍵を、デバイスＩＤを用いて暗号化する。ここでは、デバイスＩＤを用いて対応する生成鍵を暗号化する。記録部２０１が、記録媒体上に、所定の放送時間に相当するデータを記録できる容量の記録領域を複数確保し、確保した記録領域に対して順番に、データ暗号化部１０５により暗号化された所定の放送時間に相当するデジタルコンテンツと鍵暗号化部１０６により暗号化された対応する復号鍵との組を記録する。ここでは、１０分の放送時間に相当するデータを記録できる容量の記録領域をＨＤＤ上に９個確保し、９個確保した記録領域に対して順番に、生成鍵を用いて暗号化された１０分の放送時間に相当するデジタルコンテンツと暗号化された当該生成鍵との組を記録する。この時、先に記録された組が有る場合には、データを上書きする。

【００８８】逐次無効化部２０３が、新しいデータの上

書きによって無効化されなかった部分に意味のないデータを上書きするなどして、無効化すべきデータの全てを逐次破壊する。再生部１１０によるデジタルコンテンツの逐次再生を止める。

（７）実施の形態１の図３の（９）に同じ（ステップＳ９）。

（８）停止指示を受け付けると（ステップＳ９：Ｙｅｓ）、受信部１０２、デスクランブル部１０３、個別鍵生成部１０４、データ暗号化部１０５、鍵暗号化部１０６、記録部２０１の各処理を停止して蓄積動作を終了し、完全無効化部２０４が、破壊されずに残っているデータを全て破壊して停止状態に戻る（ステップＳ２２）。

（９）～（１０）実施の形態１の図３の（１１）～（１２）に同じ（ステップＳ１１～Ｓ１２）。

（１１）実施の形態１の図３の（１５）に同じ（ステップＳ１５）。

（１２）停止指示を受け付けると（ステップＳ１５：Ｙｅｓ）、受信部１０２、デスクランブル部１０３、個別鍵生成部１０４、データ暗号化部１０５、鍵暗号化部１０６、記録部２０１、鍵復号部１０８、データ復号部１０９、再生部１１０の各処理を停止してタイムシフト動作を終了し、完全無効化部２０４が、破壊されずに残っているデータを全て破壊して停止状態に戻る（ステップＳ２３）。

（１３）～（１４）実施の形態１の図３の（１７）～（１８）に同じ（ステップＳ１７～ステップＳ１８）。

【００８９】以上のように、本発明の実施の形態２によれば、複製品の生成が禁止されたデジタルコンテンツに対して、一時記録してタイムシフト視聴を許しながらも、新しいデータを記録することで所定時間前のデータを削除し記録物を逐次無効化することができるので、複製品を許さないという趣旨を逸脱せずにユーザの利便性を向上させることができると同時に、逐次無効化の処理を追加しているにも関わらず装置の負荷がほとんど増えない。

【００９０】（実施の形態３）

＜概要＞本発明の実施の形態３は、複製品を一世代だけ許すという趣旨のデジタルコンテンツを受信して記録媒体に記録した場合において、他の記録媒体に移動を許すが、移動元の記録媒体上にデジタルコンテンツが残らないように、少しづつコピーしては逐次無効化するするものである。

【００９１】＜構成＞本発明の実施の形態３に係る受信再生無効化装置のハードウエア構成は、実施の形態１と同様である。ただしマイコン８０４に、以下の機能を追加する。ユーザが複製品を一世代だけ許すという趣旨の情報が添付されたデジタルコンテンツを受信してＨＤＤ９０５に記録した場合において、マイコン８０４はＨＤＤ９０５に記録された暗号化されたデジタルコンテンツを、所定の再生時間の分毎に、コピーすると同時にコピー元のＨＤＤ９０５内の暗号化されたデジタルコンテンツを再生できないように順次無効化する。

【００９２】図７は、本発明の実施の形態３に係る受信再生無効化装置の機能ブロック図である。図７に示す受信再生無効化装置３００は、ユーザインタフェイス部１０１、受信部１０２、デスクランブル部１０３、個別鍵生成部１０４、データ暗号化部１０５、鍵暗号化部１０６、記録部１０７、鍵復号部１０８、データ復号部１０９、再生部１１０、移動部３０１、無効化判断部３０２、処理能力判断部１１２、逐次無効化部１１３、完全無効化部１１４を備える。ここで実際には、受信部１０２の機能は図１の受信装置９０２の機能に相当し、デスクランブル部１０３の機能は図１のトランスポートストリームデコーダ８０１の機能に相当し、個別鍵生成部１０４、データ暗号化部１０５、鍵暗号化部１０６、記録部１０７、鍵復号部１０８、データ復号部１０９の機能は図１の暗号エンジン８０３の機能に相当し、再生部１１０はの機能は図１のＡＶデコーダ８０２の機能に相当し、移動部３０１、無効化判断部３０２、処理能力判断部１１２、逐次無効化部１１３、完全無効化部１１４の機能は図１のマイコン８０４の機能に相当する。

【００９３】なお、実施の形態１と同様の構成要素には同じ番号を付し、その説明を省略する。移動部３０１は、先に記録媒体に記録された組を順次他の記録媒体に移動する。ここでいう移動とは、データを他の記録媒体にコピーしたのち、元の記録媒体上のデータ部分はそのままで、データの管理情報のみをデータが消去されている状態に書き換えることを指す。ここでは、ＨＤＤに記録された組を順次他の記録媒体に移動するものとする。

【００９４】無効化判断部３０２は、複製品を一世代だけ許すデジタルコンテンツであるのもかかわらず一旦記録された後で他の記録媒体に記録された組を対象として、所定の条件に基づいて無効化すべきか否かを判断する。ここでは、１０分の放送時間に相当する暗号化されたデジタルコンテンツと暗号化された生成鍵との組単位で、無効化すべきか否かを判断する。

【００９５】ここで、無効化判断部３０２による無効化すべき判断の条件は、移動部３０１により移動された事である。

＜動作＞図８は、本発明の実施の形態３に係る受信再生無効化装置の動作の一例を示す図である。

【００９６】以下に図８を用いて、本発明の移動及び無効化の動作を説明する。ここでは、実施の形態１の様な動作により、コピー制御情報「Ｃｏｐｙ　ｏｎｅ　Ｇｅｎｅｒａｔｉｏｎ」が添付されスクランブルされたデジタルコンテンツが受信されて記録される事により、所定の放送時間に相当する暗号化されたデジタルコンテンツと暗号化された生成鍵との組が複数、コピー制御情報「ＣｏｐｙＮｏ　ｍｏｒｅ」が添付されてＨＤＤに記録

されているものとする。

【００９７】（１）停止状態において、ユーザインタフェイス部１０１が、何らかのデジタルコンテンツの移動指示をユーザから受け付けるまで待つ（ステップＳ３１）。

（２）デジタルコンテンツの移動指示を受け付けると（ステップＳ３１：Ｙｅｓ）、無効化判断部３０２が、移動部３０１により移動された組が、コピー制御情報「Ｃｏｐｙ　Ｎｏ　ｍｏｒｅ」が添付されている等により、コピーを許さないことを示すデジタルコンテンツであるか否かを判断する（ステップＳ３２）。

【００９８】（３）コピーを許さないことを示さないデジタルコンテンツである場合は（ステップＳ３２：Ｎｏ）、移動部３０１が、移動すべきデジタルコンテンツの全ての組を他の記録媒体に移動する（ステップＳ３３）。

（４）コピーを許さないことを示すデジタルコンテンツである場合は（ステップＳ３２：Ｙｅｓ）、移動部３０１が、移動すべきデジタルコンテンツの組の１つを他の記録媒体に移動する。ここでは、ＨＤＤに記録された１０分の放送時間に相当する組の１つを他の記録媒体に移動する。

【００９９】（５）移動部３０１により移動され、まだ無効化されていない組が所定数又は所定量だけ有るか否かを判断する（ステップＳ３５）。

（６）移動され無効化されていない組が所定数又は所定量だけ有る場合は（ステップＳ３５：Ｙｅｓ）、逐次無効化部１１３が先に記録されたうちの無効化すべきと判断された部分を逐次無効化する（ステップＳ３６）。

【０１００】（７）移動すべきデジタルコンテンツの全ての組を移動したか否かを判断する（ステップＳ３７）。

（８）全てを移動した場合は（ステップＳ３２：Ｙｅｓ）、完全無効化部１１４が、無効化すべきデータのうち、逐次無効化部１１３により逐次破壊されなかった部分のデータを全て破壊する（ステップＳ３８）。

【０１０１】以上のように、本発明の実施の形態３によれば、複製品の生成が禁止されたデジタルコンテンツに対して、移動を許しながらも、移動元のデータを逐次無効化することができるので、複製品を許さないという趣旨を逸脱せずにユーザの利便性を向上させることができる。なお、上記実施の形態１～３では、所定の放送時間に相当するデジタルコンテンツ毎に異なる暗号鍵を生成し、生成した暗号鍵を用いて所定の放送時間に相当するデジタルコンテンツをそれぞれ暗号化したが、ある程度まとまった放送時間に相当するデジタルコンテンツや連続して記録した１まとまりのデジタルコンテンツを同じ暗号鍵を用いて暗号化してもよいし、同一の記録媒体に記録されるデジタルコンテンツを記録媒体に固有の暗号鍵を用いて暗号化してもよい。

【０１０２】また、上記実施の形態１～３では、暗号化されたデジタルコンテンツを逐次破壊する際に対応する復号鍵のみを破壊してもよいとしたが、上述のように所定の放送時間に相当するデジタルコンテンツを暗号化する際に共通する暗号鍵を用いた場合には、共通する復号鍵を逐次破壊すると同じ復号鍵を使用する他のデジタルコンテンツを復号できなくなってしまうので、復号鍵は逐次破壊しないでデータそのものの一部又は全部を破壊するものとする。もちろん同じ復号鍵を使用するデジタルコンテンツを全て無効化した後にその復号鍵を破壊してもよい。

【０１０３】また、通常データはファイルとして記録され管理されるので、上記実施の形態１～３における所定の放送時間に相当するデジタルコンテンツを含む組毎に個々のファイルとして記録してもよいし、ある程度まとまった放送時間に相当するデジタルコンテンツや連続して記録した１まとまりのデジタルコンテンツを含む複数の組を同じファイルとして記録してもよい。ここで、デジタルコンテンツを無効化する際に、組毎に個々のファイルとして記録している場合にはファイル単位で無効化の処理を行えばよいが、複数の組を同じファイルとして記録している場合には、ファイルを部分的に無効化することになり、無効化された部分を誤ってアクセスしないように無効化された部分へのアクセスを制限する。例えば、通常のオペレーティングシステムに搭載されているファイルポインタのシーク制限機能を用いることによってファイルの一部分へのアクセスを制限することができる。

【０１０４】また、上記実施の形態３において、記録部２０１が記録媒体上に複数確保する各記録領域は、必ずしも連続領域でなくてもかまわない。例えば、４Mbpsの映像音声データは１０分あたり３００ＭＢにもなるので、ＨＤＤ上にこれだけの領域を連続領域として確保することは効率的ではない。従って、各記録領域はそれぞれ複数の細かな連続領域により構成されることになり、各記録領域と細かな連続領域との関係はファイルシステムが独立に管理し、ファイルシステムは各記録領域を上位のアプリケーションに対してそれぞれ連続した領域として提示してファイルポインタを用いたアクセスを実現するのである。

【０１０５】また、コンピュータに本実施の形態１～３のような動作を実行させることができるプログラムがコンピュータ読み取り可能な記録媒体に記録され、この記録媒体が流通し取り引きの対象となりうる。また、当該プログラムは、例えばネットワーク等を介して流通し、取り引きの対象となりうる。ここでコンピュータ読み取り可能な記録媒体とは、例えば、フロッピー（登録商標）ディスク、ＣＤ、ＭＯ、ＤＶＤ、メモリカード等の着脱可能な記録媒体、及び、ハードディスク、半導体メモリ等の固定記録媒体等であり、特に限定されるもので

はない。

【０１０６】

【発明の効果】本発明に係るデータ無効化装置は、一の記録媒体に記録された対象データを無効化するデータ無効化装置であって、前記対象データは複数の部分データから構成され、前記部分データ単位で前記一の記録媒体に記録された対象データを無効化すべきか否か判断する判断手段と、前記判断手段により所定数又は所定量の部分データに対して無効化すべきと判断される度に前記一の記録媒体に記録された対象データのうちの当該無効化すべきと判断された部分データを逐次無効化する逐次無効化手段とを備えることを特徴とする。

【０１０７】これによって、対象データを所定数又は所定量の部分データ毎に、所定の条件が満たされた部分データを逐次無効化することができる。従って、対象データの一時的な使用は許すが複製品の生成を禁止したり、１世代限りの複製品を許す等の場合において、禁止された複製品の生成を一時的に許す代わりにその複製品又はオリジナルを無効化することができ、複製品を許さないという趣旨を逸脱せずにユーザの利便性を向上させることができる。

【０１０８】また、逐次複製品を無効化するので、悪意ある者が動作の途中で電源を抜くなどの小細工をして複製品を残そうとしても、所定数又は所定量の部分データ分の複製品を残す事が精一杯となるため、この単位を適切に選ぶことによりセキュリティを高めることができる。また、データ無効化装置において、前記一の記録媒体は記録された各部分データの記録順序を示す順序情報を記録しており、前記判断手段は前記順序情報により示される記録順序に基づいて、先に記録された部分データから順番に無効化すべきと判断することを特徴とすることもできる。

【０１０９】これによって、先に記録された部分データから順番に無効化すべきと判断することができる。従って、先に記録された部分データから順番に無効化するので、常に新しい部分データだけを記録しておくことができる。また、データ無効化装置において、前記一の記録媒体に記録されている対象データは他の装置から連続的に送信される送信データが現在の分まで継続的に記録されているものであり、前記データ無効化装置は、さらに、前記送信データを受信する受信手段を備え、前記逐次無効化手段は、受信手段により受信された送信データを新たな部分データとし前記一の記録媒体内の前記判断手段により無効化すべきと判断された部分データが記録されている記録領域に前記新たな部分データを上書きすることにより当該新しい部分データを記録しつつ当該無効化すべきと判断された部分データを無効化することを特徴とすることもできる。

【０１１０】これによって、無効化すべきと判断された部分データが記録されている記録領域に、新たな部分データを上書きすることができる。従って、新しい部分データを記録することが無効化する処理を兼ねるので、無効化する処理が追加されたにもかかわらず装置の負荷がほとんど増加しない。また、データ無効化装置において、前記部分データはそれぞれ前記送信データの一定の送信時間分のデータであり、前記一の記録媒体には前記一定の送信時間分のデータを記録するための記録領域が規定数だけ確保されることを特徴とすることもできる。

【０１１１】これによって、一定の送信時間分のデータを記録するための記録領域を規定数だけ確保することができる。従って、各データの記録期限を一定にすることができる。また、データ無効化装置は、前記一定の送信時間分のデータが常に一定のデータ量でない場合において、前記逐次無効化手段は前記無効化すべきと判断された部分データのうち前記新たな部分データを上書きするだけでは全て上書きできない部分に、さらに、任意のデータを上書きすることを特徴とすることもできる。

【０１１２】これによって、新たな部分データを上書きするだけでは全て上書きできない部分に、さらに、任意のデータを上書きすることができる。従って、無効化すべきデータを完全に破壊できる。また、データ無効化装置において、前記逐次無効化手段は前記新たな部分データの上書きを止めた後も先に記録されている部分データを全て無効化するまでは任意のデータを継続的に上書きすることを特徴とすることもできる。

【０１１３】これによって、新たな部分データの上書きを止めた後も任意のデータを継続的に上書きすることができる。従って、先に記録されている部分データを全て破壊することができる。また、データ無効化装置において、前記一の記録媒体には記録された各部分データの記録期限を管理するための期限管理情報が記録されており、前記判断手段は前記期限管理情報に基づいて記録期限が切れた部分データを無効化すべきと判断することを特徴とすることもできる。

【０１１４】これによって、記録期限が切れた部分データを無効化すべきと判断することができる。従って、各記録期限に基づいて各部分データを無効化するので、部分データ毎に優先度を持たせる等の設定が可能となり自由度が高くなる。また、前記データ無効化装置は、さらに、前記一の記録媒体に記録された対象データを前記部分データ単位で利用する利用手段を備え、前記判断手段は、さらに、前記利用手段により利用された部分データを無効化すべきと判断することを特徴とすることもできる。

【０１１５】これによって、さらに、利用された部分データも無効化すべきと判断することができる。従って、利用された部分データも無効化するので、複製品を許さないという趣旨をより逸脱せずにユーザの利便性を向上させることができる。また、前記データ無効化装置は、さらに、前記一の記録媒体に記録された対象データを前

記部分データ単位で利用する利用手段を備え、前記判断手段は前記利用手段により利用された部分データを無効化すべきと判断することを特徴とすることもできる。

【０１１６】これによって、利用された部分データを無効化すべきと判断することができる。従って、利用された部分データを無効化するので、再生されたり、コピーや移動された部分データを逐次無効化することにより、複製品を許さないという趣旨を逸脱せずにユーザの利便性を向上させることができる。

【０１１７】また、データ無効化装置において、前記一の記録媒体に記録されている対象データは他の装置から送信されたコンテンツデータが記録されているものであり、前記送信されたコンテンツデータには前記対象データのコピーの可否を示すコピー制御情報が添付されており、前記利用手段は前記一の記録媒体に記録されたコンテンツデータを前記部分データ単位で再生するものであり、前記判断手段は前記送信されたコンテンツデータに添付されていたコピー制御情報がコピー不可を示していた場合に限り前記利用手段により再生された部分データに対応する前記一の記録媒体に記録された部分データを無効化すべきと判断をすることを特徴とすることもできる。

【０１１８】これによって、コピー制御情報がコピー不可を示していた場合に限り、部分データを無効化すべきと判断をすることができる。従って、コピー不可であるコンテンツデータに対してのみ、一時的にコピーする代わりにその複製品を無効化することできる。また、データ無効化装置において、前記一の記録媒体に記録されている対象データには前記対象データのコピーの可否を示すコピー制御情報が添付されており、前記利用手段は前記一の記録媒体に記録された対象データを前記部分データ単位で二の記録媒体に記録するものであり、前記判断手段は前記コピー制御情報がコピー不可を示している場合に限り前記利用手段により前記二の記録媒体に記録された部分データに対応する前記一の記録媒体に記録された部分データを無効化すべきと判断をすることを特徴とすることもできる。

【０１１９】これによって、コピー制御情報がコピー不可を示している場合に限り、部分データを無効化すべきと判断をすることができる。従って、コピー不可であるコンテンツデータに対してのみ、一時的にコピーする代わりにそのオリジナルを無効化することできる。また、データ無効化装置において、前記逐次無効化手段は、前記一の記録媒体上の前記判断手段により無効化すべきと判断された部分データを全て逐次破壊することを特徴とすることもできる。

【０１２０】これによって、無効化すべきと判断された部分データを全て逐次破壊することができる。従って、セキュリティを高めることができる。また、データ無効化装置において、前記逐次無効化手段は、前記一の記録媒体上の前記判断手段により無効化すべきと判断された部分データのうちの部分データを利用する際に他のデータを利用するために先に必要となるデータを少なくとも逐次破壊することを特徴とすることもできる。

【０１２１】これによって、他のデータを利用するために先に必要となるデータを、少なくとも逐次破壊することができる。従って、装置の負荷の増大を最小限に抑えつつ、データを利用不能にすることができる。また、データ無効化装置において、前記一の記録媒体に記録されている対象データはＩピクチャーを含むＭＰＥＧデータであり、前記先に必要となるデータはＩピクチャーであることを特徴とすることもできる。

【０１２２】これによって、先に必要となるデータをＭＰＥＧデータ中のＩピクチャーとすることができる。従って、ＢピクチャーやＰピクチャーが残っていても参照すべきＩピクチャーが破壊されていれば何の役にも立たたず、Ｉピクチャー以外のＢピクチャーやＰピクチャー等を破壊しなければその分装置の負荷の増大を抑えることができる。

【０１２３】また、データ無効化装置において、前記一の記録媒体に記録されている対象データはＩピクチャーを含むＭＰＥＧデータであり、前記先に必要となるデータはＩピクチャーの先頭のセクタであることを特徴とすることもできる。これによって、先に必要となるデータをＭＰＥＧデータ中のＩピクチャーの先頭のとすることができる。

【０１２４】従って、Ｉピクチャーを正常に再生できなくなり、さらにはＢピクチャーやＰピクチャーが残っていても参照すべきＩピクチャーが正常に再生されなければ何の役にも立たたず、残りの部分を破壊しなければその分装置の負荷の増大を抑えることができる。また、データ無効化装置において、前記逐次無効化手段は、自身の処理能力に余裕が無い場合には前記少なくとも逐次破壊するとした部分のデータのみを逐次破壊することを特徴とすることもできる。

【０１２５】これによって、自身の処理能力に余裕が無い場合には少なくとも逐次破壊するとした部分のデータのみを逐次破壊することができる。従って、装置の負荷の増大を抑えつつ、セキュリティも高めることができる。また、データ無効化装置において、前記逐次無効化手段は、自身の処理能力の余裕の範囲で前記少なくとも破壊するとした部分以外のデータを破壊することを特徴とすることもできる。

【０１２６】これによって、自身の処理能力の余裕の範囲で少なくとも破壊するとした部分以外のデータを破壊することができる。従って、装置の負荷の増大を抑えつつ、セキュリティも高めることができる。また、前記データ無効化装置は、さらに、前記無効化すべきと判断された部分データのうち前記逐次無効化手段により逐次破壊されなかった部分のデータを前記処理能力に余裕があ

る時に全て破壊する完全無効化手段を備えることを特徴とすることもできる。

【０１２７】逐次無効化手段により逐次破壊されなかった部分のデータを、処理能力に余裕がある時に全て破壊することができる。従って、装置の負荷の増大を抑えつつ、セキュリティも高めることができる。また、データ無効化装置において、前記一の記録媒体に記録されている対象データは前記部分データ毎に個別の部分データ暗号鍵を用いて暗号化されており、前記一の記録媒体には暗号化され記録された各部分データを復号するための各部分データ復号鍵が記録されており、前記逐次無効化手段は、前記一の記録媒体上の前記判断手段により無効化すべきと判断された部分データに対応する部分データ復号鍵を少なくとも逐次破壊することを特徴とすることもできる。

【０１２８】これによって、部分データ復号鍵を少なくとも逐次破壊することができるので、暗号化された各部分データが記録媒体上に残っていても復号することができないので役に立たない。従って、装置の負荷の増大を最小限に抑えつつ、データを利用不能にすることができる。

【０１２９】また、前記データ無効化装置は、さらに、暗号化された前記対象データを入手する入手手段と、入手手段により入手された暗号化された対象データを正当な使用者に予め配布された使用者鍵を用いて復号し対象データを生成する復号手段と、前記部分データ毎に任意の部分データ暗号鍵と対応する部分データ復号鍵とを生成する鍵生成手段と、復号手段により復号された対象データを前記部分データ毎に鍵生成手段により生成された部分データ暗号鍵を用いて対応する部分データ復号鍵によって復号可能に暗号化するデータ暗号化手段と、鍵生成手段により生成された部分データ復号鍵を当該データ無効化装置に固有の識別子を用いて暗号化する鍵暗号化手段と、データ暗号化手段により暗号化された部分データと対応する鍵暗号化手段により暗号化された部分データ復号鍵とを前記一の記録媒体に記録する記録手段とを備えることを特徴とすることもできる。

【０１３０】これによって、暗号化された対象データを使用者鍵を用いて復号し、部分データ毎に部分データ暗号鍵を用いて独自に暗号化し、また、部分データ復号鍵を装置に固有の識別子を用いて暗号化し、これらを記録媒体に記録することができる。従って、記録されたデータは、装置に固有の識別子を用いなければ復号できず、他の装置で利用することができないので、セキュリティを高めることができる。

【０１３１】また、前記データ無効化装置は、少なくとも、前記復号手段、前記鍵生成手段、前記データ暗号化手段、及び、鍵暗号化手段を同一の半導体チップ内に収めることを特徴とすることもできる。これによって、前記復号手段、前記鍵生成手段、前記データ暗号化手段、及び、鍵暗号化手段が同一の半導体チップ内に収められるため、暗号化されていない状態の対象データが回路基盤の配線上に出てこない。

【０１３２】従って、不正に対象データを得ようとする者が処理の途中から暗号化されていない状態の対象データを容易に取り出すことができないので、セキュリティを高めることができる。本発明に係るデータ無効化プログラムは、一の記録媒体に記録された対象データを無効化するデータ無効化プログラムであって、前記対象データは複数の部分データから構成され、コンピュータに、前記部分データ単位で前記一の記録媒体に記録された対象データを無効化すべきか否か判断する判断ステップと、前記判断ステップにより所定数又は所定量の部分データに対して無効化すべきと判断される度に前記一の記録媒体に記録された対象データのうちの当該無効化すべきと判断された部分データを逐次無効化する逐次無効化ステップとを実行させることを特徴とする。

【０１３３】これによって、対象データを所定数又は所定量の部分データ毎に、所定の条件が満たされた部分データを逐次無効化することができる。従って、対象データの一時的な使用は許すが複製品の生成を禁止したり、１世代限りの複製品を許す等の場合において、禁止された複製品の生成を一時的に許す代わりにその複製品又はオリジナルを無効化することができ、複製品を許さないという趣旨を逸脱せずにユーザの利便性を向上させることができる。

【０１３４】また、逐次複製品を無効化するので、悪意ある者が動作の途中で電源を抜くなどの小細工をして複製品を残そうとしても、所定数又は所定量の部分データ分の複製品を残す事が精一杯となるため、この単位を適切に選ぶことによりセキュリティを高めることができる。また、データ無効化プログラムにおいて、前記一の記録媒体は記録された各部分データの記録順序を示す順序情報を記録しており、前記判断ステップは前記順序情報により示される記録順序に基づいて先に記録された部分データから順番に無効化すべきと判断することを特徴とすることもできる。

【０１３５】これによって、先に記録された部分データから順番に無効化すべきと判断することができる。従って、先に記録された部分データから順番に無効化するので、常に新しい部分データだけを記録しておくことができる。また、データ無効化プログラムにおいて、前記一の記録媒体に記録されている対象データは他の装置から連続的に送信される送信データが現在の分まで継続的に記録されているものであり、前記データ無効化プログラムは、さらに、コンピュータに、前記送信データを受信する受信ステップを実行させ、前記逐次無効化ステップは、受信ステップにより受信された送信データを新たな部分データとし前記一の記録媒体内の前記判断ステップにより無効化すべきと判断された部分データが記録され

ている記録領域に前記新たな部分データを上書きすることにより当該新しい部分データを記録しつつ当該無効化すべきと判断された部分データを無効化することを特徴とすることもできる。

【０１３６】これによって、無効化すべきと判断された部分データが記録されている記録領域に、新たな部分データを上書きすることができる。従って、新しい部分データを記録することが無効化する処理を兼ねるので、無効化する処理が追加されたにもかかわらず装置の負荷がほとんど増加しない。また、データ無効化プログラムにおいて、前記一の記録媒体には記録された各部分データの記録期限を管理するための期限管理情報が記録されており、前記判断ステップは前記期限管理情報に基づいて記録期限が切れた部分データを無効化すべきと判断することを特徴とすることもできる。

【０１３７】これによって、記録期限が切れた部分データを無効化すべきと判断することができる。従って、各記録期限に基づいて各部分データを無効化するので、部分データ毎に優先度を持たせる等の設定が可能となり自由度が高くなる。また、前記データ無効化プログラムは、さらに、コンピュータに、前記一の記録媒体に記録された対象データを前記部分データ単位で利用する利用ステップを実行させ、前記判断ステップは、さらに、前記利用ステップにより利用された部分データを無効化すべきと判断することを特徴とすることもできる。

【０１３８】これによって、さらに、利用された部分データも無効化すべきと判断することができる。従って、利用された部分データも無効化するので、複製品を許さないという趣旨をより逸脱せずにユーザの利便性を向上させることができる。また、前記データ無効化プログラムは、さらに、コンピュータに、前記一の記録媒体に記録された対象データを前記部分データ単位で利用する利用ステップを実行させ、前記判断ステップは前記利用ステップにより利用された部分データを無効化すべきと判断することを特徴とすることもできる。

【０１３９】これによって、利用された部分データを無効化すべきと判断することができる。従って、利用された部分データを無効化するので、再生されたり、コピーや移動された部分データを逐次無効化することにより、複製品を許さないという趣旨を逸脱せずにユーザの利便性を向上させることができる。

【０１４０】また、データ無効化プログラムにおいて、前記逐次無効化ステップは、前記一の記録媒体上の前記判断ステップにより無効化すべきと判断された部分データを全て逐次破壊することを特徴とすることもできる。これによって、無効化すべきと判断された部分データを全て逐次破壊することができる。

【０１４１】従って、セキュリティを高めることができる。また、データ無効化プログラムにおいて、前記逐次無効化ステップは、前記一の記録媒体上の前記判断手段により無効化すべきと判断された部分データのうちの部分データを利用する際に他のデータを利用するために先に必要となるデータを少なくとも逐次破壊することを特徴とすることもできる。

【０１４２】これによって、他のデータを利用するために先に必要となるデータを、少なくとも逐次破壊することができる。従って、装置の負荷の増大を最小限に抑えつつ、データを利用不能にすることができる。また、データ無効化プログラムにおいて、前記一の記録媒体に記録されている対象データは前記部分データ毎に個別の部分データ暗号鍵を用いて暗号化されており、前記一の記録媒体には暗号化され記録された各部分データを復号するための各部分データ復号鍵が記録されており、前記逐次無効化ステップは、前記一の記録媒体上の前記判断手段により無効化すべきと判断された部分データに対応する部分データ復号鍵を少なくとも逐次破壊することを特徴とすることもできる。

【０１４３】これによって、部分データ復号鍵を少なくとも逐次破壊することができるので、暗号化された各部分データが記録媒体上に残っていても復号することができないので役に立たない。従って、装置の負荷の増大を最小限に抑えつつ、データを利用不能にすることができる。

【０１４４】本発明に係るデータ無効化方法は、一の記録媒体に記録された対象データを無効化するデータ無効化方法であって、前記対象データは複数の部分データから構成され、前記部分データ単位で前記一の記録媒体に記録された対象データを無効化すべきか否か判断する判断ステップと、前記判断ステップにより所定数又は所定量の部分データに対して無効化すべきと判断される度に前記一の記録媒体に記録された対象データのうちの当該無効化すべきと判断された部分データを逐次無効化する逐次無効化ステップとを備えることを特徴とする。

【０１４５】これによって、対象データを所定数又は所定量の部分データ毎に、所定の条件が満たされた部分データを逐次無効化することができる。従って、対象データの一時的な使用は許すが複製品の生成を禁止したり、１世代限りの複製品を許す等の場合において、禁止された複製品の生成を一時的に許す代わりにその複製品又はオリジナルを無効化することができ、複製品を許さないという趣旨を逸脱せずにユーザの利便性を向上させることができる。

【０１４６】また、逐次複製品を無効化するので、悪意ある者が動作の途中で電源を抜くなどの小細工をして複製品を残そうとしても、所定数又は所定量の部分データ分の複製品を残す事が精一杯となるため、この単位を適切に選ぶことによりセキュリティを高めることができる。また、データ無効化方法において、前記一の記録媒体は記録された各部分データの記録順序を示す順序情報を記録しており、前記判断ステップは前記順序情報によ

り示される記録順序に基づいて、先に記録された部分データから順番に無効化すべきと判断することを特徴とすることもできる。

【０１４７】これによって、先に記録された部分データから順番に無効化すべきと判断することができる。従って、先に記録された部分データから順番に無効化するので、常に新しい部分データだけを記録しておくことができる。また、データ無効化方法において、前記一の記録媒体に記録されている対象データは他の装置から連続的に送信される送信データが現在の分まで継続的に記録されているものであり、前記データ無効化方法は、さらに、前記送信データを受信する受信ステップを備え、前記逐次無効化ステップは、受信ステップにより受信された送信データを新たな部分データとし前記一の記録媒体内の前記判断ステップにより無効化すべきと判断された部分データが記録されている記録領域に前記新たな部分データを上書きすることにより当該新しい部分データを記録しつつ当該無効化すべきと判断された部分データを無効化することを特徴とすることもできる。

【０１４８】これによって、無効化すべきと判断された部分データが記録されている記録領域に、新たな部分データを上書きすることができる。従って、新しい部分データを記録することが無効化する処理を兼ねるので、無効化する処理が追加されたにもかかわらず装置の負荷がほとんど増加しない。また、データ無効化方法において、前記一の記録媒体には記録された各部分データの記録期限を管理するための期限管理情報が記録されており、前記判断ステップは前記期限管理情報に基づいて記録期限が切れた部分データを無効化すべきと判断することを特徴とすることもできる。

【０１４９】これによって、記録期限が切れた部分データを無効化すべきと判断することができる。従って、各記録期限に基づいて各部分データを無効化するので、部分データ毎に優先度を持たせる等の設定が可能となり自由度が高くなる。また、前記データ無効化方法は、さらに、前記一の記録媒体に記録された対象データを前記部分データ単位で利用する利用ステップを備え、前記判断ステップは、さらに、前記利用ステップにより利用された部分データを無効化すべきと判断することを特徴とすることもできる。

【０１５０】これによって、さらに、利用された部分データも無効化すべきと判断することができる。従って、利用された部分データも無効化するので、複製品を許さないという趣旨をより逸脱せずにユーザの利便性を向上させることができる。また、前記データ無効化方法は、さらに、前記一の記録媒体に記録された対象データを前記部分データ単位で利用する利用ステップを備え、前記判断ステップは前記利用ステップにより利用された部分データを無効化すべきと判断することを特徴とすることもできる。

【０１５１】これによって、利用された部分データを無効化すべきと判断することができる。従って、利用された部分データを無効化するので、再生されたり、コピーや移動された部分データを逐次無効化することにより、複製品を許さないという趣旨を逸脱せずにユーザの利便性を向上させることができる。

【０１５２】また、データ無効化方法において、前記逐次無効化ステップは、前記一の記録媒体上の前記判断ステップにより無効化すべきと判断された部分データを全て逐次破壊することを特徴とすることもできる。これによって、無効化すべきと判断された部分データを全て逐次破壊することができる。

【０１５３】従って、セキュリティを高めることができる。また、データ無効化方法において、前記逐次無効化ステップは、前記一の記録媒体上の前記判断手段により無効化すべきと判断された部分データのうちの部分データを利用する際に他のデータを利用するために先に必要となるデータを少なくとも逐次破壊することを特徴とすることもできる。

【０１５４】これによって、他のデータを利用するために先に必要となるデータを、少なくとも逐次破壊することができる。従って、装置の負荷の増大を最小限に抑えつつ、データを利用不能にすることができる。また、データ無効化方法において、前記一の記録媒体に記録されている対象データは前記部分データ毎に個別の部分データ暗号鍵を用いて暗号化されており、前記一の記録媒体には暗号化され記録された各部分データを復号するための各部分データ復号鍵が記録されており、前記逐次無効化ステップは、前記一の記録媒体上の前記判断手段により無効化すべきと判断された部分データに対応する部分データ復号鍵を少なくとも逐次破壊することを特徴とすることもできる。

【０１５５】これによって、部分データ復号鍵を少なくとも逐次破壊することができるので、暗号化された各部分データが記録媒体上に残っていても復号することができないので役に立たない。従って、装置の負荷の増大を最小限に抑えつつ、データを利用不能にすることができる。

【図面の簡単な説明】

【図１】本発明の実施の形態１に係る受信再生無効化装置のハードウエア構成の一例を示す図である。

【図２】本発明の実施の形態１に係る受信再生無効化装置の機能ブロック図である。

【図３】本発明の実施の形態１に係る受信再生無効化装置の動作の一例を示す図である。

【図４】本発明の実施の形態１に係る受信再生無効化装置の動作の別の例を示す図である。

【図５】本発明の実施の形態２に係る受信再生無効化装置の機能ブロック図である。

【図６】本発明の実施の形態２に係る受信再生無効化装

置の動作の一例を示す図である。

【図７】本発明の実施の形態３に係る受信再生無効化装置の機能ブロック図である。

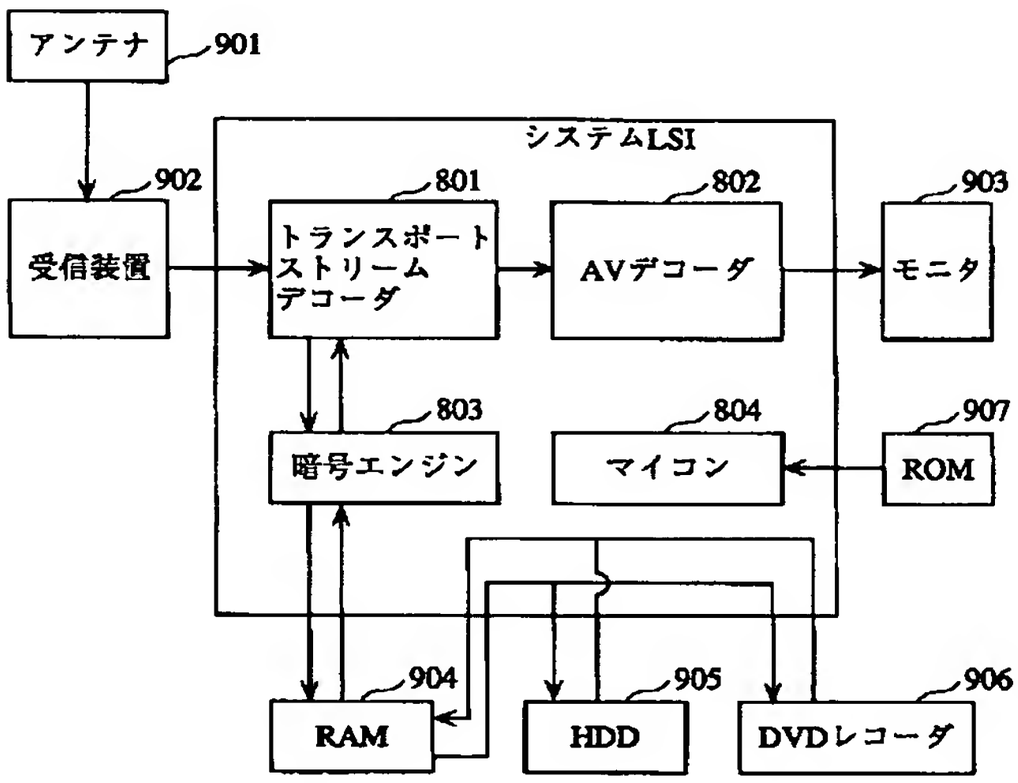
【図８】本発明の実施の形態３に係る受信再生無効化装置の動作の一例を示す図である。

【符号の説明】

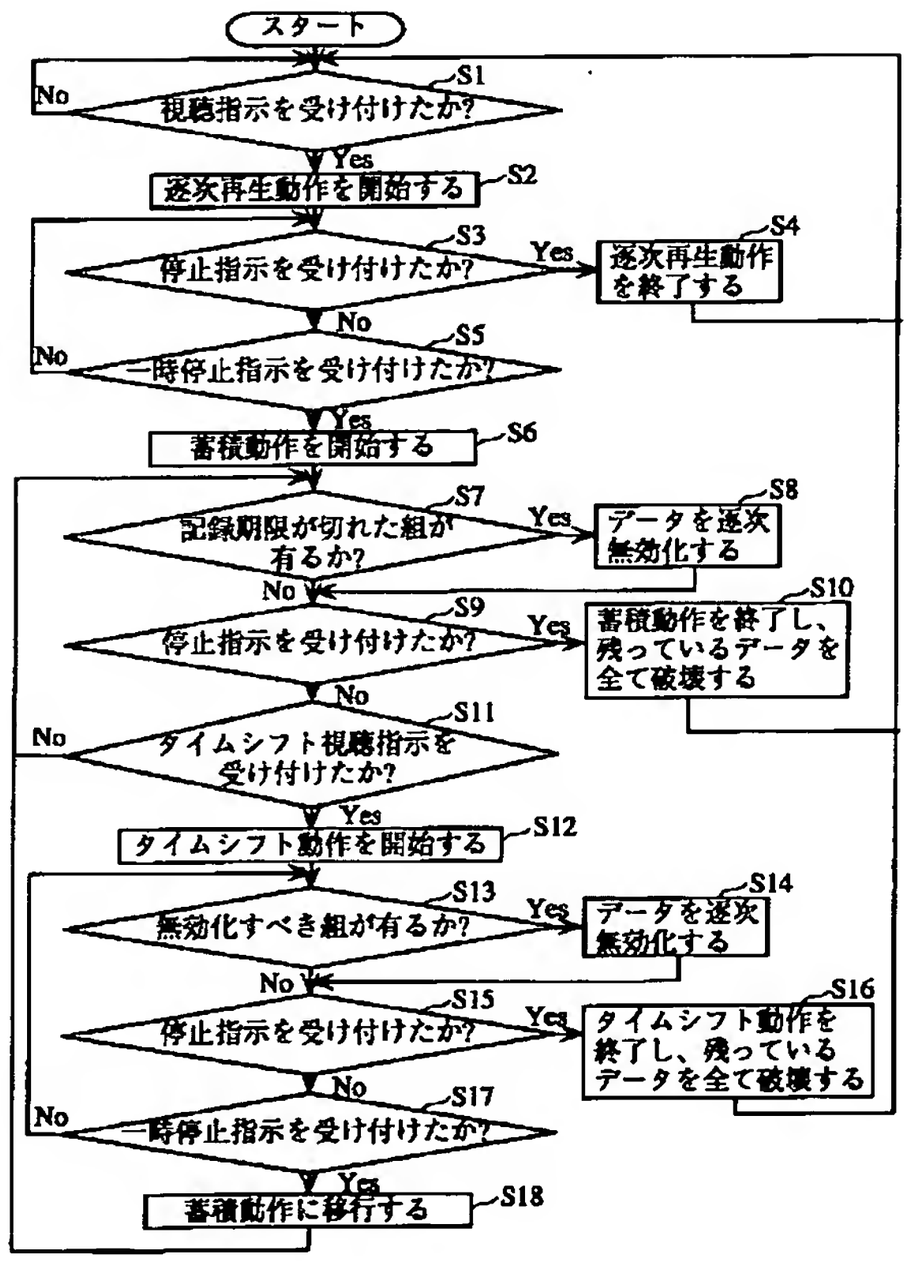
１００　受信再生無効化装置
１０１　ユーザインタフェイス部
１０２　受信部
１０３　デスクランブル部
１０４　個別鍵生成部
１０５　データ暗号化部
１０６　鍵暗号化部
１０７　記録部
１０８　鍵復号部
１０９　データ復号部
１１０　再生部

＊１１１　無効化判断部
１１２　処理能力判断部
１１３　逐次無効化部
１１４　完全無効化部
２００　受信再生無効化装置
２０１　記録部
２０２　無効化判断部
２０３　逐次無効化部
２０４　完全無効化部
３００　受信再生無効化装置
３０１　移動部
３０２　無効化判断部
８００　システムＬＳＩ
８０１　トランスポートストリームデコーダ
８０２　ＡＶデコーダ
８０３　暗号エンジン
＊８０４　マイコン

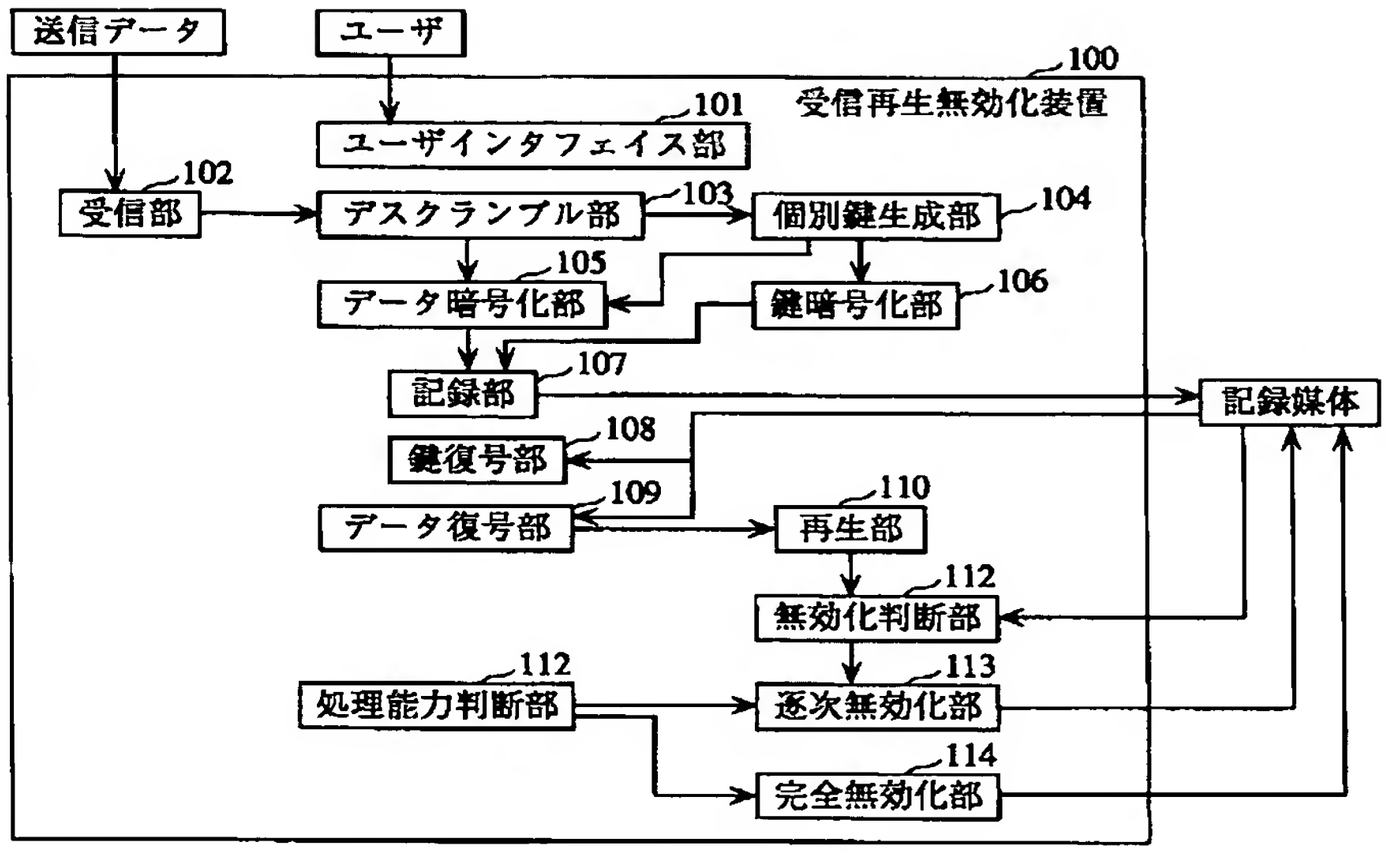
【図１】



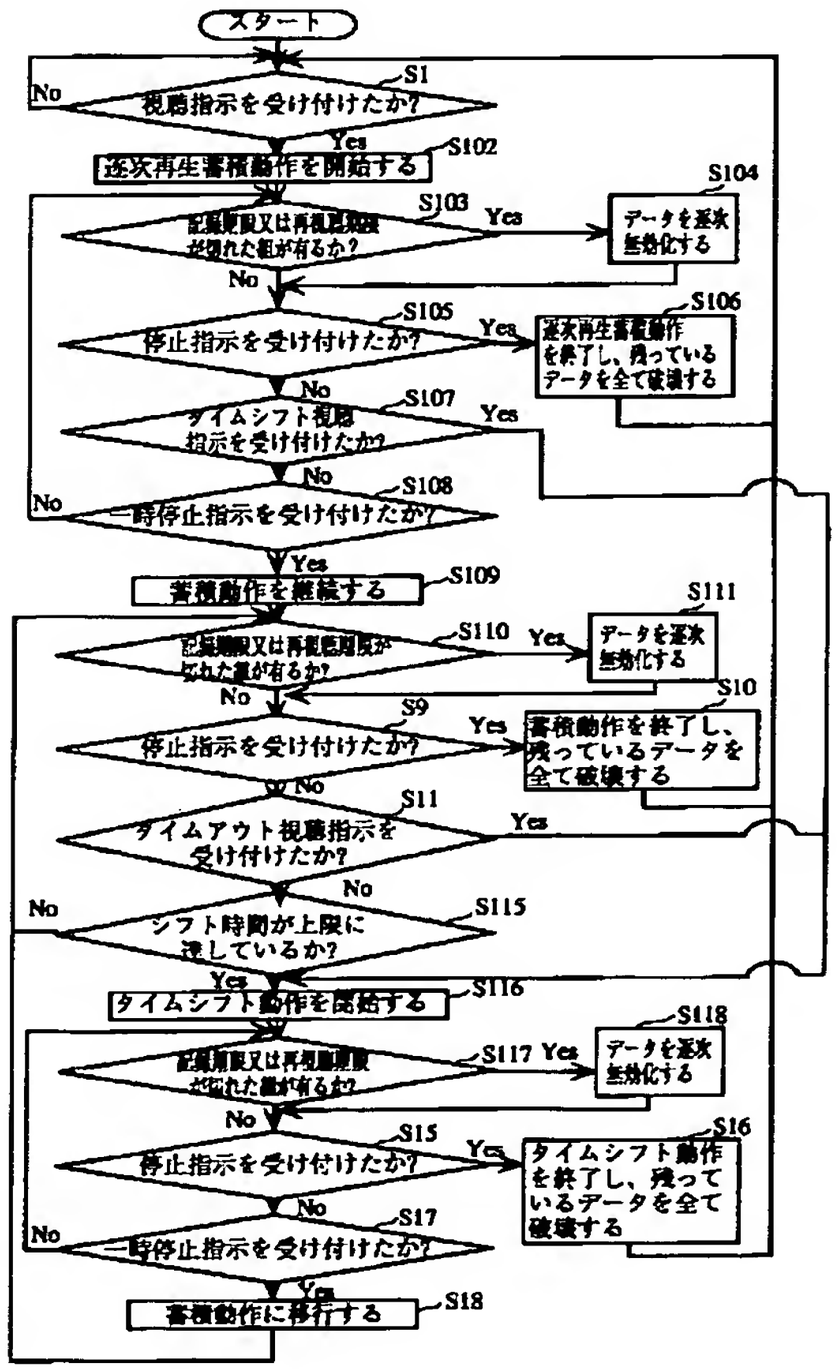
【図３】



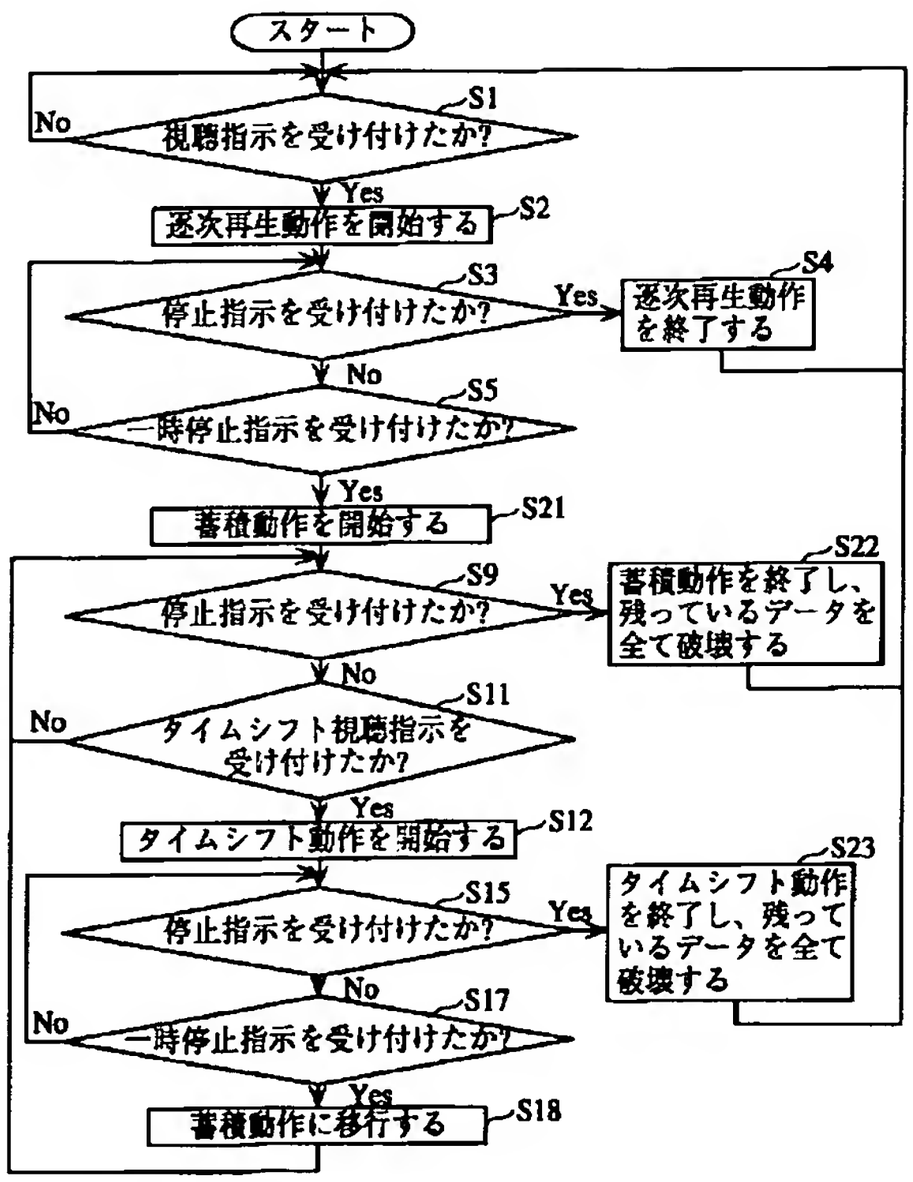
【図２】


送信データ
ユーザ
100
受信再生無効化装置
101
ユーザインタフェイス部
102
受信部
デスクランブル部
103
個別鍵生成部
104
データ暗号化部
105
鍵暗号化部
106
記録部
107
記録媒体
鍵復号部
108
データ復号部
109
再生部
110
無効化判断部
112
処理能力判断部
113
逐次無効化部
114
完全無効化部

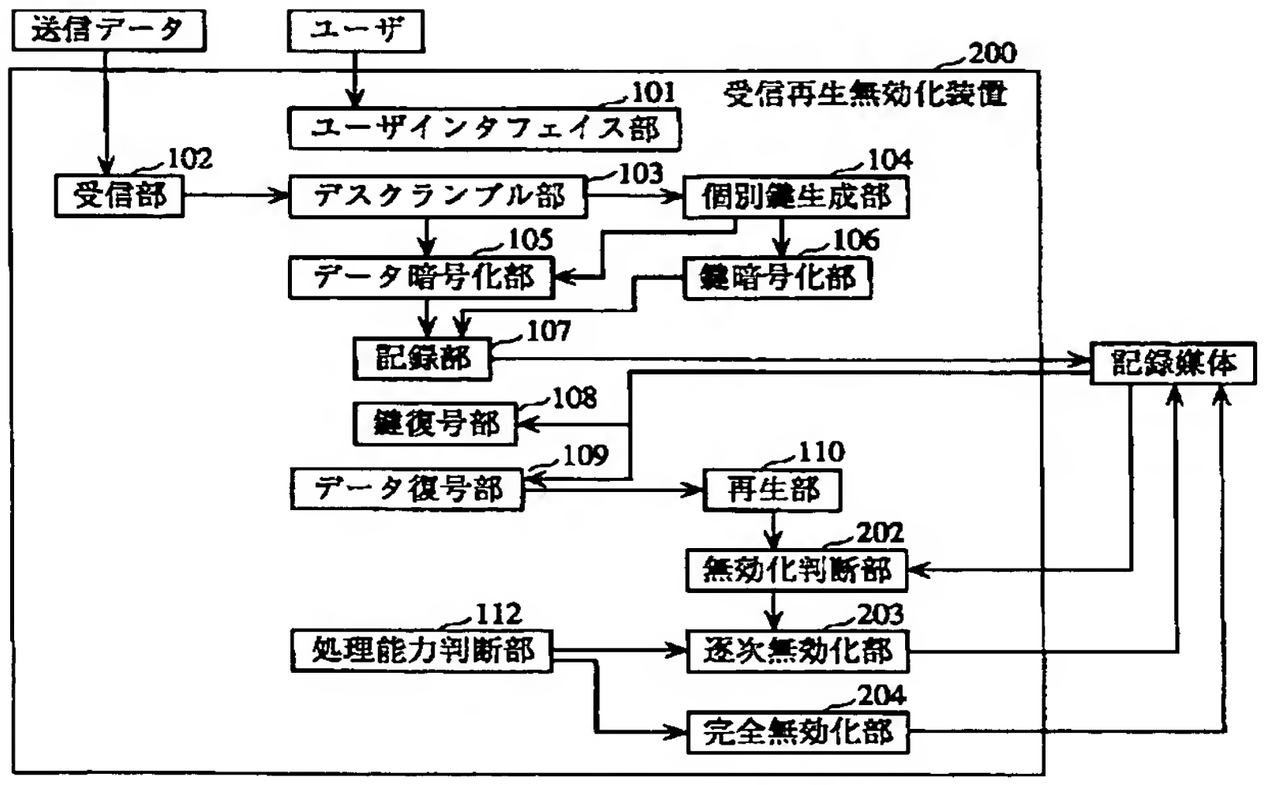
【図４】


スタート
S1
No
視聴指示を受け付けたか?
Yes
S102
逐次再生蓄積動作を開始する
S104
S103
Yes
データを逐次無効化する
No
S105
停止指示を受け付けたか?
Yes
S106
逐次再生蓄積動作を終了し、残っているデータを全て破壊する
No
S107
タイムシフト視聴指示を受け付けたか?
Yes
No
S108
No
一時停止指示を受け付けたか?
Yes
S109
蓄積動作を継続する
S111
S110
Yes
データを逐次無効化する
No
S10
S9
Yes
蓄積動作を終了し、残っているデータを全て破壊する
No
S11
タイムアウト視聴指示を受け付けたか?
Yes
No
S115
No
シフト時間が上限に達しているか?
Yes
S116
タイムシフト動作を開始する
S118
S117
Yes
データを逐次無効化する
No
S15
停止指示を受け付けたか?
Yes
S16
タイムシフト動作を終了し、残っているデータを全て破壊する
No
S17
No
一時停止指示を受け付けたか?
Yes
S18
蓄積動作に移行する

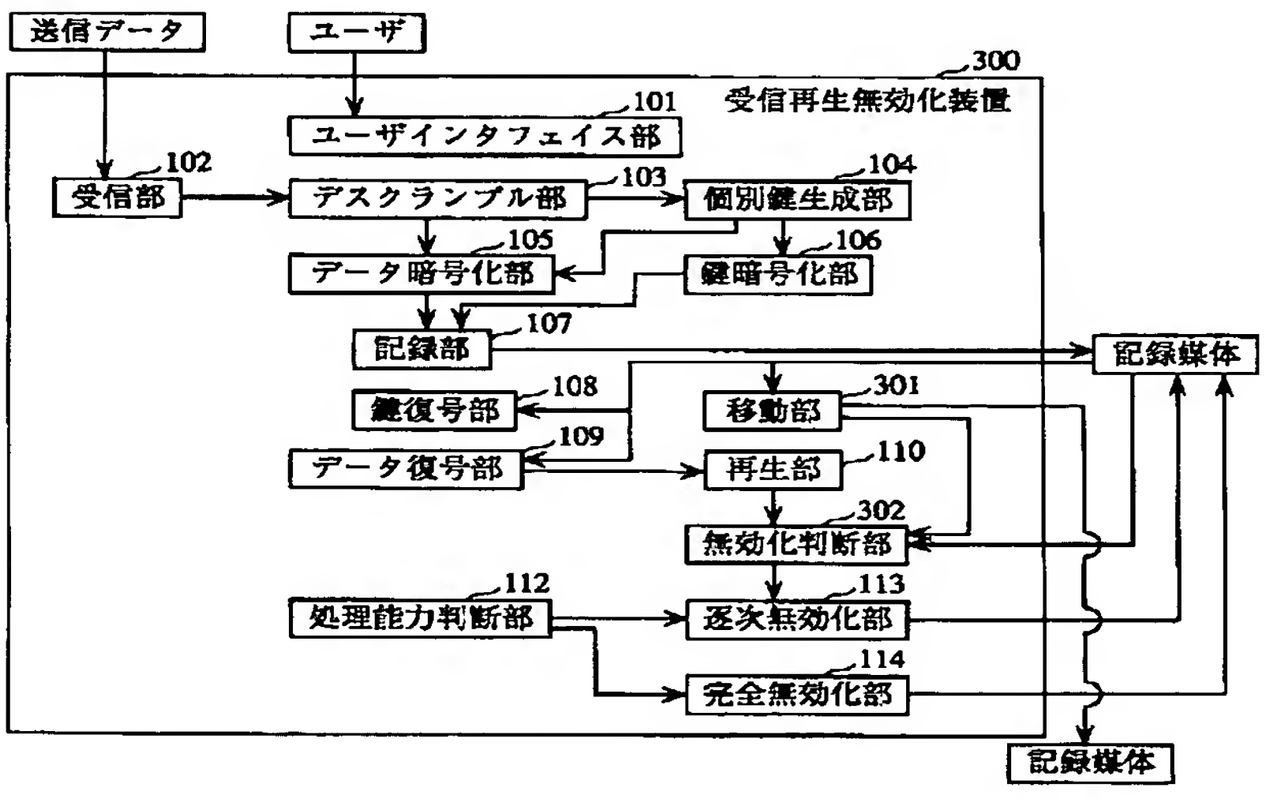
【図６】


スタート
S1
No
視聴指示を受け付けたか?
Yes
S2
逐次再生動作を開始する
S3
停止指示を受け付けたか?
Yes
S4
逐次再生動作を終了する
No
S5
No
一時停止指示を受け付けたか?
Yes
S21
蓄積動作を開始する
S22
S9
停止指示を受け付けたか?
Yes
蓄積動作を終了し、残っているデータを全て破壊する
No
S11
No
タイムシフト視聴指示を受け付けたか?
Yes
S12
タイムシフト動作を開始する
S23
S15
停止指示を受け付けたか?
Yes
タイムシフト動作を終了し、残っているデータを全て破壊する
No
S17
No
一時停止指示を受け付けたか?
Yes
S18
蓄積動作に移行する

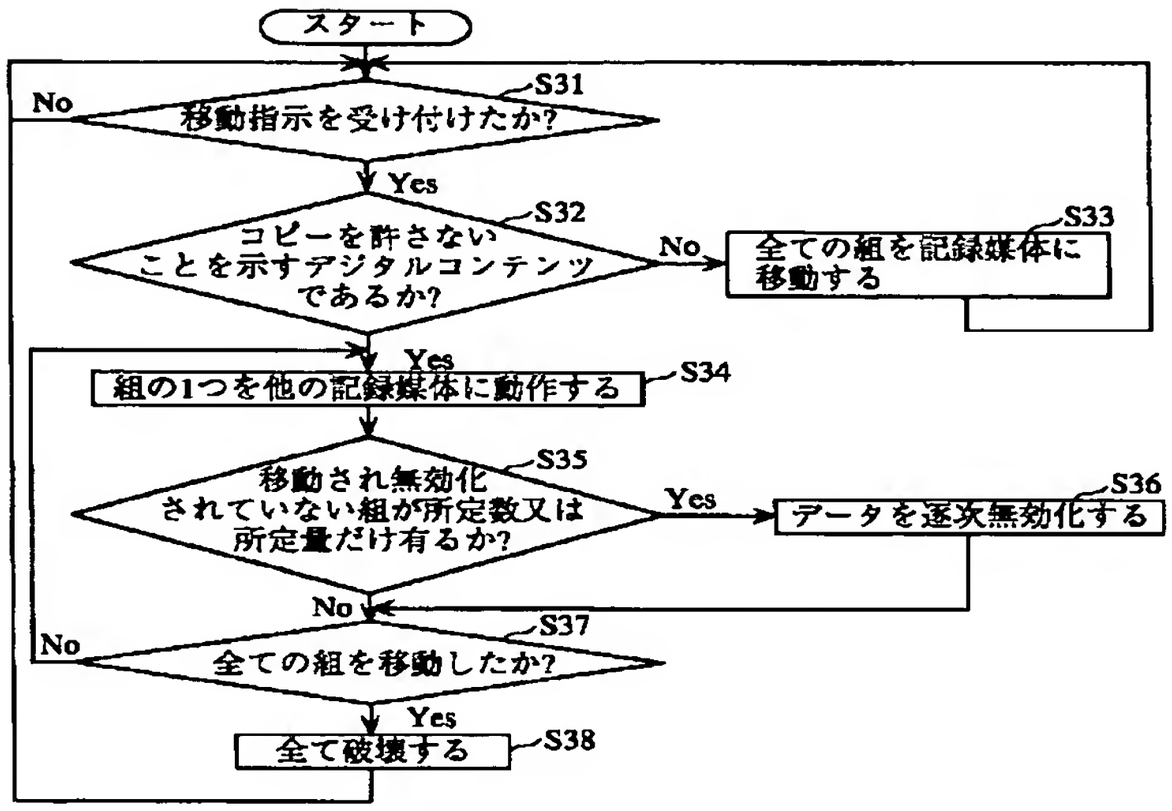
【図５】


送信データ
ユーザ
200
受信再生無効化装置
101
ユーザインタフェイス部
102
受信部
103
デスクランブル部
104
個別鍵生成部
105
データ暗号化部
106
鍵暗号化部
107
記録部
記録媒体
108
鍵復号部
109
データ復号部
110
再生部
202
無効化判断部
112
処理能力判断部
203
逐次無効化部
204
完全無効化部

【図７】


送信データ
ユーザ
300
受信再生無効化装置
101
ユーザインタフェイス部
102
受信部
103
デスクランブル部
104
個別鍵生成部
105
データ暗号化部
106
鍵暗号化部
107
記録部
記録媒体
108
鍵復号部
301
移動部
109
データ復号部
110
再生部
302
無効化判断部
112
処理能力判断部
113
逐次無効化部
114
完全無効化部
記録媒体

【図８】



フロントページの続き

(51)Int.Cl.[7]		識別記号	F I		テーマコード(参考)
Ｈ０４Ｎ	5/781		Ｈ０４Ｎ	5/781	５１０Ｆ
	5/85			5/91	Ｐ
	5/91				

(72)発明者　宮▲ざき▼　雅也
大阪府門真市大字門真1006番地　松下電器
産業株式会社内

Ｆターム(参考)　5B017 AA07 BA07 BA08 BB10 CA16
5C052 AA02 AB03 AB04 CC06 DD10
5C053 FA13 FA23 FA24 GB06 JA21
KA24 LA07
5J104 NA02 PA14